III. DROIT AU RESPECT DE LA VIE PRIVÉE ET À LA PROTECTION DES DONNÉES EN LIEN AVEC LES TECHNOLOGIES DE L'INFORMATION

Coline Fievet[511], Loïck Gerard[512], Noémie Gillard[513], Manon Knockaert[514], Alejandra Michel[515], Julie Mont[516], Karen Rosier[517], Thomas Tombal[518], Odile Vanreck[519]

Sous la coordination de Karen Rosier

112. Introduction. La présente chronique s'inscrit dans la continuité des précédentes chroniques publiées au sein de la *R.D.T.I.* et couvrant respectivement les périodes 2002 à 2008[520], 2009 à 2011[521], 2012 à 2014[522].

Depuis le début des années nonante, la matière de la protection des données à caractère personnel est régie, en droit belge, par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[523] (ci-après loi du 8 décembre 1992). Suite à l'adoption, au niveau européen, de la directive 95/46/CE[524], la loi du 8 décembre 1992 a été largement remaniée par une loi du 11 décembre 1998[525]. L'année 2018 marque un nouveau tournant dans la matière de la protection des données puisque, le 25 mai 2018, le règlement général sur la protection des données (ci-après RGPD) entre en application dans tous les États membres et constitue donc le nouveau texte de référence en cette matière. La présente chronique s'attarde sur les décisions prises par les juridictions belges et de l'Union européenne entre 2015 et 2017, et relatives à la directive 95/46/CE et à la loi du 8 décembre 1992[526].

Sous ce titre sont regroupées les analyses de jurisprudence relatives à l'application de la législation en matière de protection des données à caractère personnel (A) et quelques questions spéciales relatives aux communications électroniques en lien avec la protection des données (B)[527]. Elle

511 Chercheuse au Centre de Recherche Information, Droit et Société de l'Université de Namur (CRIDS).
512 Chercheur au CRIDS.
513 Chercheuse au CRIDS et avocate au barreau de Liège.
514 Chercheuse au CRIDS.
515 Chercheuse au CRIDS.
516 Chercheuse au CRIDS et avocate au barreau de Namur.
517 Chercheuse Senior au CRIDS, Maître de conférences à l'Université de Namur, avocate au barreau du Brabant wallon.
518 Chercheur au CRIDS.
519 Chercheuse au CRIDS et avocate au barreau du Brabant wallon.
520 « Libertés », *R.D.T.I.*, 2009/2, n° 35, pp. 81-126.
521 « Libertés et société de l'information », *R.D.T.I.*, 2012/3-4, n° 48, pp. 68-127.
522 « Libertés et société de l'information », *R.D.T.I.*, 2015/2-3, n° 59, pp. 71-114.
523 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, pp. 5801 et s.
524 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, 23 novembre 1995, pp. 31 et s.
525 Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999, pp. 3049 et s.
526 La présente chronique n'intègre pas systématiquement les arrêts de la Cour européenne des droits de l'homme qui touchent à la protection des données. Un résumé thématique de ces arrêts est accessible sur le site www.echr.coe.int (fiches thématiques du service de presse).
527 Des décisions se rattachant plus spécifiquement aux communications électroniques dans le domaine de la recherche et poursuite des infractions sont analysées sous le titre V « Criminalité informatique ».

intègre également l'analyse de la jurisprudence relative à l'usage des technologies de l'information et de la communication dans les relations de travail (C) ainsi qu'un état des lieux des principales décisions rendues par la Commission de la protection de la vie privée à propos de l'e-gouvernement (D).

A. Protection des données à caractère personnel

1. Champ d'application matériel (Thomas Tombal)

113. Traitement automatisé de données ou traitement non automatisé de données contenues dans un fichier. Lors de la période couverte par la présente chronique, les juridictions belges ont, par deux fois, été confrontées à la problématique du champ d'application matériel 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[528] (ci-après, loi du « 8 décembre 1992 » ou « loi vie privée »). Ces deux décisions ont été rendues dans le cadre d'une même affaire, à l'origine de laquelle une banque avait erronément et automatiquement enclenché une procédure d'enregistrement de retard de paiement auprès de la Banque nationale de Belgique, entrainant le fichage et l'altération de la capacité d'emprunt de son client[529].

La cour d'appel de Liège a rejeté l'application de la loi vie privée, estimant que les contrats bancaires en cause ne pouvaient être qualifiés de « fichiers » au sens de la loi[530]. Saisie d'un pourvoi à l'encontre de cet arrêt, la Cour de cassation adhérera au raisonnement de la juridiction d'appel, en précisant que, « en l'absence de fichier tel que défini à l'article 1er de la loi du 8 décembre 1992, celle-ci ne trouve pas à s'appliquer »[531]. Force est de constater que ces arrêts procèdent d'une lecture partielle et erronée du champ d'application de la loi vie privée[532]. En effet, l'article 3, § 1er, de cette loi dispose que celle-ci s'applique « à tout traitement de données à caractère personnel automatisé en tout ou en partie, *ainsi qu'*à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». La notion de fichier n'est donc pertinente que dans l'hypothèse où aucun moyen automatisé n'est employé pour le traitement[533]. À l'inverse, dès l'instant où il est recouru, en tout ou en partie, à des moyens automatisés, la loi vie privée sera applicable[534]. En l'espèce, « l'évident recours à des moyens numériques dans le monde bancaire suffisait à rendre la loi vie privée applicable »[535].

528 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.

529 C. de Terwangne, « La difficile application de la législation de protection des données à caractère personnel », obs. sous Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, p. 752.

530 Liège (6e ch. corr.), 13 octobre 2016, R.G. no 2015/IC/9, inédit, www.juridat.be.

531 Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, p. 751, note C. de Terwangne.

532 C. de Terwangne, « La difficile application de la législation de protection des données à caractère personnel », obs. sous Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, p. 752.

533 *Ibid.*, p. 753.

534 *Ibid.*

535 *Ibid.*

2. Questions de droit international privé (Thomas Tombal)

a. Compétence juridictionnelle

114. Cookies Facebook – Référé – Compétence des juridictions belges. Dans une affaire en référé opposant la Commission de la protection de la vie privée belge (ci-après « C.P.V.P. ») à Facebook[536], relative au traçage des internautes belges par le biais de cookies et de plug-ins sociaux[537], le président du tribunal de première instance néerlandophone de Bruxelles s'est déclaré compétent tant à l'égard de Facebook Belgium que de Facebook Inc. et de Facebook Ireland Ltd[538]. Pour ce faire, le juge des référés a procédé à un raisonnement mêlant des questions de compétence internationale et de droit applicable[539]. Ainsi, estimant que la loi belge était applicable sur le fondement de l'article 4.1.a) de la directive 95/46/CE[540], celui-ci en déduit que « le juge belge dispose ainsi d'un pouvoir de juridiction international pour statuer sur la présente demande, et applique de surcroît la législation belge »[541].

Ce raisonnement n'a pas été suivi par la cour d'appel de Bruxelles, qui, réformant la décision, a estimé, pour sa part, ne pas disposer de la compétence internationale à l'égard de Facebook Inc. et Facebook Ireland Ltd[542]. La cour écarte, en effet, de façon systématique et détaillée, les différents fondements juridiques avancés par la C.P.V.P. pour établir la compétence des juridictions belges.

Premièrement, la cour précise qu'elle ne peut fonder sa compétence internationale sur la base des articles 4 et 28 de la directive 95/46/CE, dès lors que celle-ci n'a pas d'effet direct[543]. Qui plus est, la cour ajoute qu'aucune de ces deux dispositions ne peuvent fonder la compétence juridictionnelle d'une juridiction d'un État membre, dès lors que l'article 4 détermine uniquement la question du droit applicable[544] et que l'article 28 sert uniquement à préciser la compétence des autorités de contrôle nationales[545]. La cour précise également que les arrêts *Google Spain*[546] et *Weltimmo*[547] de la Cour de justice de l'Union européenne (ci-après « C.J.U.E. »), relatifs à ces articles, ne permettent

536 Étaient parties à la cause : Facebook Inc. (USA), Facebook Ireland Limited et Facebook Belgium.

537 Pour plus de précisions sur les faits reprochés et les outils techniques employés, voy. *infra*, n^os^ 155 à 159.

538 Civ. Bruxelles (nl.) (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, n° 62, p. 91, note G. Dejemeppe ; *Juristenkrant*, 2015, n° 318, p. 3.

539 G. Dejemeppe, « L'affaire *Facebook* : questions de procédure », note sous Civ. Bruxelles (nl.) (réf.) (ord.), 9 novembre 2015 et Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 114.

540 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 281/31 du 23 novembre 1995. Sur le droit applicable, voy. *infra*, n° 117.

541 Civ. Bruxelles (nl.) (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, n° 62, p. 100.

542 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe, point 46. Cet arrêt est disponible en intégralité sur http://deeplinking.kluwer.nl/?param=00CCEC7E&cpid=WKNL-LTR-Nav2. En revanche, la cour se déclare compétente à l'égard de Facebook Belgium (point 47 de l'arrêt).

543 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. dejemeppe, points 19-20 et 27-28.

544 *Ibid.*, points 27-28.

545 *Ibid.*, points 21 et 26. Sur la compétence des autorités de contrôle nationales, voy. *infra*, n° 118.

546 C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, aff. C-131/12, EU:C:2014:317.

547 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14, EU:C:2015:639.

pas non plus de fonder la compétence des tribunaux belges, la question de la compétence juridictionnelle n'y étant nullement traitée[548].

Deuxièmement, la cour estime qu'elle ne peut fonder sa compétence internationale sur la base de l'article 32, § 3, de la loi vie privée, dès lors que cette disposition accorde simplement la qualité à agir, dans certaines hypothèses, au président de la C.P.V.P.[549].

Troisièmement, la cour considère qu'elle ne peut pas non plus fonder sa compétence internationale sur la base de l'article 35 du règlement n° 1215/2012 (Bruxelles I*bis*)[550], dès lors que le litige en l'espèce n'entrait pas dans le champ d'application matériel de ce règlement. En effet, celui-ci s'applique uniquement « en matière civile et commerciale »[551], ce qui exclut les litiges, tels qu'en l'espèce, dans lesquels une autorité publique exerce une part de la puissance publique[552]. La cour adopte le même raisonnement pour écarter l'application de l'article 10 du Code de droit international privé[553].

115. Cookies Facebook – Fond – Application du droit international public et non du droit international privé. Il convient de noter que, par un jugement du 16 février 2018, traitant du fond de l'affaire étudié au point précédent, le tribunal de première instance néerlandophone de Bruxelles établit sa compétence à l'égard de Facebook[554] sur la base de l'application de principes de droit international public[555], et non de droit international privé, dès lors que le tribunal estime que la C.P.V.P. exerce une part de la puissance publique[556]. Cette décision fera l'objet d'une analyse plus détaillée lors de la prochaine chronique de jurisprudence.

b. Droit applicable – Champ d'application territorial

116. Traitement effectué « dans le cadre des activités de l'établissement du responsable du traitement ». Dans la foulée de son arrêt *Google Spain*[557], analysé lors de la précédente chronique[558], la Cour de justice a, par ses arrêts *Weltimmo*[559] et *Verein*[560], une nouvelle fois été appelée à se prononcer sur l'interprétation à donner de l'expression « dans le cadre des activités d'un établis-

548 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe, points 23-24.

549 *Ibid.*, points 32-33.

550 Règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *J.O.C.E.* 351/1 du 20 décembre 2012.

551 *Ibid.*, art. 1er.

552 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe, point 39.

553 *Ibid.*, point 44.

554 Facebook Inc., Facebook Ireland Limited et Facebook Belgium.

555 Le tribunal applique ces principes de concert avec les articles 4 et 28 de la directive 95/46, et les articles 3*bis* et 32, § 3, de la loi vie privée.

556 Civ. Bruxelles (24e ch. N.), 16 février 2018, R.G. n° 2016/153/A, inédit, points 12, 19 et 20.

557 C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, précité.

558 Voy. C. Burnet, M. Piron, B. Losdyck, O. Vanreck, J.-M. Van Gyseghem, E. Degrave, C. Gayrel, J. Herveg et K. Rosier, « Libertés et société de l'information », *R.D.T.I.*, 2015, n° 59-60, p. 88.

559 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14, EU:C:2015:639.

560 C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, aff. C-191/15, EU:C:2016:612.

sement du responsable du traitement », contenue à l'article 4.1.a) de la directive 95/46/CE[561]. Sont également pertinentes, à cet égard, les conclusions rendues par l'avocat général Y. Bot dans l'affaire *Wirtschaftsakademie*[562].

La première affaire concernait l'exploitation par la société Weltimmo, immatriculée en Slovaquie, d'un site internet d'annonces immobilières concernant des biens situés en Hongrie, ce qui impliquait le traitement, par cette société, de données à caractère personnel des annonceurs hongrois[563]. La seconde était relative aux conditions générales d'Amazon.de, lesquelles contenaient une clause précisant que, lorsque cela est justifié, cette société peut vérifier et évaluer les données à caractère personnel des clients et procéder à un échange de données avec d'autres entreprises au sein du groupe Amazon[564]. Dans la troisième, l'autorité régionale allemande de protection des données de Schleswig-Holstein (ci-après l'« ULD ») reprochait à la Wirtschaftsakademie, société allemande spécialisée dans le domaine de l'éducation, de collecter, grâce à des cookies et via une « page fan » hébergée sur le site Facebook[565], les données personnelles des utilisateurs sans les en informer[566].

Dans ces affaires, il fut tout d'abord rappelé que le législateur européen avait délibérément opté pour un champ d'application territorial large, de sorte que l'expression « dans le cadre des activités de l'établissement du responsable du traitement » ne pouvait être interprétée restrictivement[567]. Fut ensuite réalisée une analyse en deux temps des composantes de cette expression. Dans un premier temps, il a été rappelé que la forme juridique de l'établissement n'est pas déterminante et que seul importe « l'exercice effectif et réel d'une activité au moyen d'une installation stable »[568]. L'évaluation de l'existence d'un tel établissement ne doit donc pas être purement formaliste (lieu d'enregistrement), mais doit plutôt être dynamique et casuistique, au regard du degré de stabilité de l'installation et de la réalité de l'exercice des activités, compte tenu de la nature des activités et des prestations[569]. Ainsi, cette notion « s'étend à toute activité réelle et effective, même

561 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 281/31 du 23 novembre 1995.

562 Conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, ECLI:EU:C:2017:796. L'arrêt de la Cour de justice rendu dans le courant de l'année 2018 sera analysé lors de la prochaine chronique de jurisprudence (C.J.U.E., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16).

563 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 9.

564 C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, précité, point 30.

565 Sont ici impliquées, les sociétés Facebook Inc., Facebook Ireland Limited et Facebook Germany GmbH (chargée de la promotion et de la vente d'espaces publicitaires et d'autres activités de marketing destinées aux habitants d'Allemagne).

566 Conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 3.

567 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, points 25-27 ; conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 87.

568 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 28 ; conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 90.

569 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 29 ; C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, précité, point 77 ; conclusions de l'avocat

minime, exercée au moyen d'une installation stable »[570]. La Cour précisa toutefois, dans son arrêt *Verein*, qu'un « tel établissement ne saurait exister [dans un État membre] du simple fait que le site internet de l'entreprise en question y est accessible »[571]. Dans un second temps, il fut reprécisé que le traitement en question doit être effectué « non pas "par" l'établissement concerné lui-même, mais uniquement "dans le cadre des activités" de celui-ci »[572].

Au vu de ce qui précède, la Cour conclut, dans l'arrêt *Weltimmo*, qu'un État membre, autre que celui dans lequel le responsable de traitement est enregistré, peut appliquer son droit national à ce responsable, pour autant que ce dernier exerce « au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué »[573]. Dans son arrêt *Verein*, la Cour conclut que le traitement « est régi par le droit de l'État membre vers lequel une entreprise dirige ses activités s'il s'avère que cette entreprise procède au traitement des données en question dans le cadre des activités d'un établissement situé dans cet État membre »[574]. Enfin, l'avocat général Y. Bot suggéra de conclure, quant à lui, que le traitement « est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre lorsqu'une entreprise exploitant un réseau social crée dans cet État membre une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par cette entreprise et dont l'activité vise les habitants de cet État membre »[575]. Dans son arrêt du 5 juin 2018, la Cour a substantiellement suivi ce raisonnement[576].

117. Cookies Facebook – Droit applicable. Dans l'affaire en référé opposant la C.P.V.P. à Facebook, évoquée précédemment[577], le président du tribunal de première instance néerlandophone de Bruxelles se fonda sur l'article 4.1.a) de la directive 95/46/CE[578] et sur une application par analogie de la jurisprudence *Google Spain*[579], pour établir l'application de la loi belge, estimant que « le traitement de données à caractère personnel en question est effectué dans le

général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, points 89 et 90.

570 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 31 ; C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, précité, point 75 ; conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 89.

571 C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, précité, point 76.

572 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 35 ; C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, précité, point 78 ; conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 91.

573 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 41.

574 C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, précité, point 81.

575 Conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 127.

576 C.J.U.E., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, point 60. Cet arrêt sera analysé lors de la prochaine chronique de jurisprudence.

577 Voy. *supra*, n° 114.

578 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 281/31 du 23 novembre 1995.

579 C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, précité.

cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire belge (…) de sorte que les activités de Facebook Belgium sont pour cette raison indissociablement liées aux activités de l'exploitant du réseau social »[580]. N'est ainsi pas pertinent, pour le juge des référés, l'argument de Facebook selon lequel « Facebook Belgium ne traite pas elle-même les données à caractère personnel et ne conclurait pas elle-même les contrats avec les annonceurs »[581].

Soulignons que la cour d'appel n'a pas été appelée à se prononcer sur cette question du droit applicable, dès lors qu'elle s'était déclarée incompétente à l'égard de Facebook Inc. et de Facebook Ireland Ltd[582]. En revanche, par son jugement du 16 février 2018, traitant du fond de l'affaire, le tribunal de première instance néerlandophone de Bruxelles a suivi le même raisonnement que le juge des référés[583]. Cette dernière décision fera l'objet d'une analyse plus détaillée lors de la prochaine chronique de jurisprudence.

118. Droit applicable et compétence des autorités de contrôle nationales. Dans les affaires *Weltimmo*[584] et *Wirtschaftsakademie*[585] précitées[586], se posait également la question de l'articulation entre droit applicable et compétence des autorités de contrôle nationales.

Ainsi, dans l'affaire *Weltimmo*, la juridiction de renvoi hongroise désirait savoir si – dans l'hypothèse où le droit applicable au traitement des données ne serait pas le droit hongrois, mais le droit slovaque –, l'article 28, §§ 1er, 3 et 6, de la directive 95/46/CE permettait néanmoins à l'autorité de contrôle hongroise d'exercer certains pouvoirs lui étant spécifiquement accordés par la loi hongroise de transposition[587]. Plus précisément, se posait la question de savoir si, en ce cas, l'autorité de contrôle hongroise pouvait tout de même sanctionner un responsable de traitement établi en Slovaquie en lui infligeant une amende[588].

Pour répondre à cette question, la Cour rappela tout d'abord qu'en vertu de l'article 28, § 6, de la directive 95/46/CE, « chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément à l'article 28, § 3, et ce, indépendamment du droit national applicable »[589]. Cependant, la Cour ajouta que, dans l'hypothèse où le droit applicable serait celui d'un autre État membre, les pouvoirs de l'autorité de contrôle ne comprendront pas nécessairement « l'ensemble de ceux dont elle est investie conformément au droit de l'État membre dont elle relève »[590]. Ceci se justifie en vertu des « exigences résultant de la souveraineté territoriale de l'État membre concerné, du principe de légalité et de

580 Civ. Bruxelles (nl) (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, n° 62, p. 100.
581 *Ibid.*
582 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe, point 46. Voy. *supra*, n° 114.
583 Civ. Bruxelles (24e ch. N.), 16 février 2018, R.G. n° 2016/153/A, inédit, points 19 et 20.
584 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14, EU:C:2015:639.
585 Conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, ECLI:EU:C:2017:796.
586 Voy. *supra*, n° 116.
587 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, précité, point 43.
588 *Ibid.*, points 49 et 59. Le droit hongrois accorde en effet, à la différence du droit slovaque, un tel pouvoir de sanction à l'autorité de contrôle hongroise.
589 *Ibid.*, point 52.
590 *Ibid.*, point 55.

la notion d'État de droit »[591]. Ce faisant, si l'autorité de contrôle nationale conclut que le droit d'un autre État membre est applicable, elle ne pourra imposer de sanctions en dehors du territoire de l'État membre dont elle relève, et devra prendre contact avec l'autorité de contrôle de cet autre État membre, via le mécanisme de coopération prévu à l'article 28, § 6, de la directive, pour que cette dernière sanctionne elle-même le responsable de traitement – pour autant que le droit de cet autre État membre le permette[592]. *In casu*, si le droit slovaque s'avère être applicable, l'autorité de contrôle hongroise ne pourra donc pas exercer les pouvoirs de sanction lui étant spécifiquement confiés par la loi hongroise de transposition[593].

Dans l'affaire *Wirtschaftsakademie* soumise à la Cour de justice, se pose la question de savoir si, à considérer que le droit applicable est celui de l'État membre dont relève l'autorité de contrôle (le droit allemand), cette autorité (l'ULD) est en mesure d'exercer directement ses pouvoirs à l'encontre de Facebook Ireland Ltd, ou si, au contraire, l'article 28, § 6, de la directive 95/46 lui impose de demander à l'autorité de contrôle irlandaise d'exercer ses pouvoirs à l'encontre de cette société[594]. En substance, l'avocat général Y. Bot est d'avis que l'ULD « peut exercer l'intégralité des pouvoirs effectifs d'intervention qui lui ont été conférés conformément à l'article 28, § 3, à l'encontre du responsable du traitement, y compris lorsque ce responsable est établi dans un autre État membre ou bien dans un État tiers »[595]. Il ajoute que l'ULD « est habilitée à exercer ses pouvoirs d'intervention à l'encontre de ce responsable de manière autonome et sans être tenue d'appeler préalablement l'autorité de contrôle de l'État membre dans lequel est situé ledit responsable à exercer ses pouvoirs »[596]. Dans son arrêt du 5 juin 2018, la Cour a substantiellement suivi ce raisonnement. Elle a estimé que « lorsqu'une entreprise établie en dehors de l'Union européenne dispose de plusieurs établissements dans différents États membres, l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de la directive 95/46/CE à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre » et que « cette autorité de contrôle est compétente pour apprécier, de manière autonome par rapport à l'autorité de contrôle de ce dernier État membre, la légalité d'un tel traitement de données et peut exercer ses pouvoirs d'intervention à l'égard de l'organisme établi sur son territoire sans préalablement appeler l'autorité de contrôle de l'autre État membre à intervenir »[597].

3. Définitions des notions clés (Odile Vanreck)

119. Données à caractère personnel. La donnée à caractère personnel est définie par l'article 1, § 1er, de la loi du 8 décembre 1992, reprenant quasiment à l'identique la définition de l'article 2, a), de la directive 95/46/CE, comme « toute information concernant une personne physique identifiée ou identifiable désignée ci-après "personne concernée"; est réputée identi-

591 *Ibid.*, point 56.
592 *Ibid.*, points 57 et 60.
593 *Ibid.*, point 59.
594 Conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité, point 36.
595 *Ibid.*, point 128.
596 *Ibid.*, point 136.
597 C.J.U.E., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, § 75. Cet arrêt sera davantage commenté dans la prochaine chronique.

fiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

Durant la période concernée par la présente chronique, les juridictions belges ont reconnu comme étant des données à caractère personnel :

- les données recueillies au moyen d'un appareil photo digital et par lesquelles un excès de vitesse litigieux avait été constaté[598] ;
- les images enregistrées par un détective privé[599] ainsi que le rapport de ce détective[600] ;
- les informations contenues dans le cookie Datr enregistré par Facebook (à savoir la combinaison d'un identifiant unique et d'informations additionnelles telles que l'adresse IP et l'URL du site web visité) permettant de surveiller le comportement de navigation de l'internaute lorsque celui-ci visite une page web du domaine facebook.com[601] ;
- les données d'identification du propriétaire et du titulaire de la plaque d'immatriculation d'un véhicule ainsi que le numéro de la plaque d'immatriculation[602].

La Cour de justice a, quant à elle, jugé que constituaient des données à caractère personnel :

- des données fiscales, notamment des données relatives aux revenus déclarés[603] ou des données, telles que le nom de personnes physiques, reprises sur une liste de personnes considérées comme des prête-noms[604] ;
- des indications relatives à l'identité des personnes, telles que l'identité des personnes qui, en tant qu'organe légal d'une société ou membre d'un tel organe, ont le pouvoir d'engager la société à l'égard des tiers et de la représenter en justice et qui participent à l'administration, à

598 Cass., 26 mai 2015, R.G. n° P.14.0069.N, disponible sur www.juridat.be.

599 C. trav. Bruxelles, 18 mai 2015, R.G. n° 2014/AB/996, disponible sur www.juridat.be ; C. trav. Bruxelles, 9 juin 2017, R.G. n° 2014/AB/279, disponible sur www.juridat.be. Voy. aussi C. trav. Liège, 6 février 2015, R.G. n° 2013/AL/392, disponible sur www.juridat.be.

600 C. trav. Bruxelles, 9 juin 2017, R.G. n° 2014/AB/279, disponible sur www.juridat.be. Dans cette affaire, la cour du travail a précisé que les données collectées par le détective privé ne constituaient pas des données relatives à la santé, bien qu'elles étaient « relatives aux activités d'une personne et aux moyens utilisés par elle pour se déplacer » et qu'elles pouvaient « être utilisées par d'autres personnes pour faire des déductions relatives à sa santé ». Dans le cas d'espèce, ces informations avaient été soumises « au médecin expert chargé par la cour de donner un avis sur l'état de santé de monsieur K.B. (état antérieur, lésions et répercussions de celles-ci) ». La cour a ensuite indiqué que, même si les informations étaient relatives à la santé de la personne concernée, un tel traitement serait autorisé puisqu'il entre dans le champ d'application des exceptions à l'interdiction de traitement des données relatives à la santé.

601 Civ. Bruxelles (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016, n° 62, p. 91. Le tribunal rappelle que « [t]ant la Cour de justice de l'UE que le Groupe de travail Article 29 ont déjà explicitement confirmé que les adresses IP constituent des "données à caractère personnel" (…) ». Cette décision a été réformée par la cour d'appel de Bruxelles, dans un arrêt du 29 juin 2016, pour des motifs touchant à la compétence du tribunal. Nous renvoyons à cet égard au n° 114 dans la présente chronique.

602 Cass. (2e ch. N), 13 décembre 2016, *R.D.T.I.*, n° 2016, n° 65, p. 63. Dans cet arrêt, la Cour de cassation se fondait sur la définition de données à caractère personnel prévue à l'article 2, 10°, de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules, qui définit la donnée à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement ».

603 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a. c. Președintele Casei Naționale de Asigurări de Sănătate e.a.*, aff. C-201/14, EU:C:2015:638, § 29. Sur cet arrêt, voy. également les nos 135 et 139 dans la présente chronique.

604 C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy*, aff. C-73/16, § 41.

la surveillance et au contrôle de la société ainsi que l'identité des liquidateurs et leurs pouvoirs respectifs[605]. Par cet arrêt, la Cour rappelle sa jurisprudence selon laquelle « la circonstance que ces informations s'inscrivent dans le contexte d'une activité professionnelle n'est pas de nature à leur ôter la qualification de données à caractère personnel »[606] ;

– une adresse de protocole internet (adresse IP) dynamique[607] enregistrée par un fournisseur de services de médias en ligne lors de la consultation par un visiteur de son site internet lorsque ce fournisseur dispose de moyens légaux lui permettant de faire identifier ce visiteur grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet[608].

Dans cette affaire *Breyer*, la Cour précise qu'« une adresse IP dynamique ne constitue pas une information se rapportant *directement*[609] à une personne physique identifiée, dans la mesure où une telle adresse ne révèle pas directement l'identité de la personne physique propriétaire de l'ordinateur à partir duquel la consultation d'un site internet a lieu ni celle d'une autre personne qui pourrait utiliser cet ordinateur »[610].

La Cour s'attache ensuite à déterminer si cette adresse IP dynamique peut constituer, dans les circonstances de l'espèce, une donnée à caractère personnel. Elle rappelle qu'une personne identifiable est une personne qui peut être identifiée de manière directe, mais également indirecte, de sorte qu'« il n'est pas nécessaire [qu'une] information permette à elle seule d'identifier la personne concernée »[611]. Faisant référence au considérant 26 de la directive 95/46[612], elle déduit que toutes les informations permettant d'identifier une personne concernée ne doivent pas être entre les mains d'une même personne pour qu'une information soit qualifiée de donnée à caractère personnel. En l'espèce, les informations supplémentaires nécessaires pour identifier la personne concernée utilisatrice du site internet ne sont pas détenues par le fournisseur de services de médias en ligne mais par le fournisseur d'accès à internet. La Cour doit alors juger si la possibilité de combiner une adresse IP dynamique avec des informations complémentaires fournies par le fournisseur d'accès à internet constitue un « moyen susceptible d'être raisonnablement mis en œuvre » pour identifier la personne concernée. En l'occurrence, en droit allemand, le fournisseur de services de médias en ligne dispose de la possibilité de s'adresser, dans certains cas, à l'autorité compétente afin que cette dernière « entreprenne les démarches nécessaires pour obtenir ces informations [supplémentaires permettant l'identification de la personne concernée] auprès du fournisseur d'accès à internet »[613]. La Cour

605 C.J.U.E., 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, aff. C-398/15, EU:C:2017:197, §§ 6 et 34.

606 *Ibid.*, § 34.

607 Une adresse IP dynamique est une adresse provisoire attribuée « à chaque connexion à internet » et remplacée « lors de connexions ultérieures ». À l'inverse, une adresse IP statique est invariable et permet « l'identification permanente du dispositif connecté au réseau ». Voy. C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14, EU:C:2016:779, § 36.

608 C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14, EU:C:2016:779, § 48. Sur cet arrêt, voy. également les n^{os} 130 et 134 dans la présente chronique.

609 Nous soulignons.

610 C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14, EU:C:2016:779, § 38.

611 *Ibid.*, § 41.

612 Considérant 26 de la directive 95/46 : « (…) pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne (…) ».

613 C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14, EU:C:2016:779, § 47.

conclut dès lors que « le fournisseur de services de médias en ligne dispose de moyen susceptible d'être raisonnablement mis en œuvre afin de faire identifier, à l'aide d'autres personnes, à savoir l'autorité compétente et le fournisseur d'accès à internet, la personne concernée sur la base des adresses IP conservées »[614] ;

– le nom ou le numéro d'identification attribué à un candidat à un examen professionnel qui est apposé sur une copie d'examen ou sur le feuillet de couverture d'une telle copie[615]. La Cour précise qu'est sans incidence « le point de savoir si l'examinateur peut ou non identifier le candidat au moment de la correction et de la notation de la copie d'examen »[616].
Dans cet arrêt *Novak*, relatif à la demande de consultation de sa copie d'un examen professionnel par un candidat, la Cour a de nouveau eu l'occasion de rappeler le principe selon lequel toutes les informations permettant l'identification d'une personne concernée ne doivent pas nécessairement être détenues par une seule personne pour qu'une donnée soit qualifiée de données à caractère personnel. En l'espèce, la Cour a indiqué que « dans l'hypothèse où l'examinateur ne connait pas l'identité du candidat lors de la notation des réponses fournies par celui-ci dans le cadre d'un examen, l'entité organisant l'examen (…) dispose en revanche des informations nécessaires lui permettant d'identifier sans difficultés ou doutes ce candidat à partir de son numéro d'identification, apposé sur la copie d'examen ou le feuillet de couverture de cette copie, et ainsi, lui attribuer ses réponses »[617] ;

– les réponses fournies par un candidat lors d'un examen professionnel ainsi que les annotations de l'examinateur y relatives[618].
Dans le cadre de cette même affaire *Novak* que nous venons d'évoquer, la Cour de justice a rappelé que la notion de données à caractère personnel n'était pas « restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci "concernent" la personne en cause », à savoir lorsque l'information est liée à cette personne[619]. La Cour a également expliqué que « la même information peut concerner plusieurs personnes physiques »[620] de sorte que le fait que les annotations de l'examinateur au sujet des réponses du candidat « constituent des informations qui, en raison de leur contenu, de leur finalité et de leur effet, sont liées à ce candidat n'est pas infirmée par le fait que ces annotations constituent également des informations concernant l'examinateur »[621].

120. Données « judiciaires »[622]. Durant la période étudiée, les tribunaux de police francophones de Bruxelles et de Liège, division Verviers, ont constaté que l'usage d'une dashcam à des fins de collecte de preuve en cas de collision impliquait des traitements de données à caractère

614 *Ibid.*, § 48.
615 C.J.U.E., 20 décembre 2017, *Peter Nowak c. Data Protection Commissioner*, aff. C-434/16, EU:C:2017:994, § 31.
616 *Ibid.*, §§ 29 et 30.
617 *Ibid.*, § 31.
618 *Ibid.*, § 42.
619 *Ibid.*, § 34.
620 *Ibid.*, § 45.
621 *Ibid.*, § 44.
622 Par cette notion, nous visons les données mentionnées à l'article 8 de la loi du 8 décembre 1992, à savoir les données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté.

personnel judiciaires[623]. Ces deux juridictions ont rappelé que le principe de l'interdiction du traitement de telles données connaît des exceptions, notamment lorsque le traitement est nécessaire pour la gestion de son propre contentieux.

121. Traitement de données à caractère personnel. Le traitement de données à caractère personnel est défini comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel »[624].

Durant la période étudiée, les juridictions belges ont mis en avant le caractère extrêmement large de cette notion, en estimant que :

- « le traitement de données obtenues au moyen d'appareils photos digitaux entraine inévitablement la communication de données »[625], une telle communication constituant un traitement de données à caractère personnel ;
- « le traitement automatisé des adresses IP et des cookies de navigateur permettant une identification (…) constituent (…) un traitement de données à caractère personnel »[626]. Le tribunal précise que « le simple enregistrement ou la simple réception automatisée de ces données du navigateur d'un utilisateur qui visite une page web dotée d'un plug-in social » constitue déjà un traitement, de sorte qu'il est sans incidence que ces données soient enregistrées pour une courte période ou de manière durable[627] ;
- l'enregistrement d'images vidéo prises par un détective privé et leur conservation[628], ainsi que la réalisation, par un détective privé, d'un rapport[629] impliquent des traitements de données à caractère personnel.

623 Pol. Bruxelles (fr.) 15 avril 2016, n° 15A664, *VAV-CRA*, 2016/3, pp. 69 et s. ; Pol. Liège (div. Verviers), 26 juin 2017, n° 16A121, *VAV-CRA*, 2017/5, pp. 36 et s.

624 Art. 1, § 2, de la loi du 8 décembre 1992. La directive 95/46/CE, en son article 2, b), propose une définition quasiment identique de cette notion.

625 Cass., 26 mai 2015, R.G. n° P.14.0069.N, disponible sur www.juridat.be.

626 Civ. Bruxelles (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, p. 104. Sur cet arrêt, voy. également les n^{os} 114, 117 et 155 à 159 dans la présente chronique.

627 *Ibid.*, p. 104.

628 C. trav. Bruxelles, 18 mai 2015, R.G. n° 2014/AB/996, disponible sur www.juridat.be ; C. trav. Bruxelles, 9 juin 2017, R.G. n° 2014/AB/279, disponible sur www.juridat.be ; C. trav. Liège, 6 février 2015, R.G. n° 2013/AL/392, disponible sur www.juridat.be.

629 C. trav. Bruxelles, 9 juin 2017, R.G. n° 2014/AB/279, disponible sur www.juridat.be ; C. trav. Liège, 6 février 2015, R.G. n° 2013/AL/392, www.juridat.be. Dans cet arrêt, la cour du travail de Liège précise que « le rapport de détective constitue bien un traitement de données à caractère personnel au sens de la loi, sauf s'il est rédigé sans aucune utilisation de l'informatique, ce qui est devenu l'exception ». Elle conclut que « la seule constatation de ce que le film que l'appelante entend produire aux débats a été gravé sur un support DVD suffit à établir que la loi du 8 décembre 1992 trouve bien à s'appliquer au présent litige ». Sur cette décision, voy. également les n^{os} 137 et 188 dans la présente chronique.

La Cour de justice de l'Union européenne a, pour sa part, indiqué que constituaient des traitements de données à caractère personnel :

- « la communication, par un établissement bancaire, des nom et adresses d'un de ses clients »[630] ;
- le transfert de données fiscales relatives aux revenus déclarés des requérants par l'agence nationale d'administration fiscale roumaine (ANAF) à la Caisse nationale de sécurité sociale (CNAS) ainsi que leur traitement ultérieur par la CNAS[631] ;
- « l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers »[632] ;
- l'inscription et la conservation d'informations relatives à l'identité de personnes physiques dans un registre et la communication de ces informations à des tiers[633] ;
- la collecte et l'utilisation, par les différentes autorités fiscales, de listes contenant le nom de certaines personnes physiques[634].

122. Fichier. L'article 1er, § 3, de la loi du 8 décembre 1992 définit le fichier comme « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ». Une définition identique est inscrite à l'article 1, c), de la directive 95/46/CE.

Cette notion était au centre d'un arrêt du 13 octobre 2016 de la cour d'appel de Liège qui a été confirmé par la Cour de cassation en date du 22 février 2017[635]. Dans cette affaire, en raison d'une erreur commise par une banque[636], un client s'est retrouvé enregistré au fichier des enregistrements non régis[637], ce qui lui avait causé un préjudice. Dans le cadre de ses discussions avec la banque, il a demandé à ce qu'une copie des contrats les liant ainsi que des informations relatives à la carte bancaire en cause lui soient communiquées. La banque refusant de répondre à ses demandes, celui-ci a lancé citation directe du chef d'infraction à plusieurs articles de la loi du 8 décembre 1992. La Cour de cassation, confirmant l'arrêt de la cour d'appel de Liège, a écarté l'application de la loi du 8 décembre 1992, estimant que cette dernière n'était pas applicable en

630 C.J.U.E., 16 juillet 2015, *Coty Germany GmbH c. Stadtsparkasse Magdeburg*, aff. C-580/13, EU:C:2015:485, disponible sur https://curia.europa.eu, § 26. Sur cet arrêt, voy. également le n° 89 dans la présente chronique.

631 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a. c. Președintele Casei Naționale de Asigurări de Sănătate e.a.*, aff. C-201/14, EU:C:2015:638, § 29.

632 C.J.U.E. (gr. ch.), 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14, EU:C:2015:650, § 45.

633 C.J.U.E., 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, aff. C-398/15, EU:C:2017:197, § 35.

634 C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy*, aff. C-73/16, § 34.

635 Liège (6e ch.), 13 octobre 2016, R.G. n° 2015/IC/9, inédit ; Cass., 22 février 2017, R.G. n° P.16.1110.F, disponible sur www.juridat.be. Sur ces arrêts, voy. également les nos 113 et 129 dans la présente chronique.

636 Erreur qui avait été reconnue par la banque.

637 Le fichier des enregistrements non régis (ENR) est une base de données gérée par la Banque nationale de Belgique sur la base de conventions entre celle-ci et des prêteurs. Les prêteurs y enregistrent les données des défauts de paiement relatifs aux contrats de crédit conclus par des personnes physiques qui ne sont pas repris dans le fichier de la Centrale des crédits aux particuliers (CCP).

raison de l'absence de fichier[638]. Comme indiqué *supra*[639], cet arrêt est illustratif d'une mauvaise compréhension du champ d'application et des notions centrales de la loi du 8 décembre 1992[640].

123. Responsable de traitement. En droit belge, le responsable du traitement est défini, à l'article 1, § 4, de la loi du 8 décembre 1992, comme « la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »[641]. Une définition semblable est comprise à l'article 2, d), de la directive 95/46/CE[642]. Le Groupe de travail Article 29 sur la protection des données[643] estime que la notion de « responsable de traitement » est une « notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle »[644].

Le Groupe de travail a établi trois types d'hypothèses permettant d'attribuer la qualité de responsable de traitement à une entité. Premièrement, le responsable de traitement peut être désigné de manière explicite dans une norme juridique nationale[645]. À titre exemplatif, la Cour constitutionnelle a mis en avant le fait que chaque commune est responsable du traitement du « fichier des personnes physiques ou morales qui ont fait l'objet d'une sanction administrative ou d'une mesure alternative (…) sur la base du règlement général de police »[646] et que la Chambre nationale des huissiers de justice est considérée comme le responsable du traitement pour ce qui concerne le registre central des actes authentiques dématérialisés des huissiers de justice[647]. Deuxièmement, la qualité de responsable de traitement peut découler « de règles juridiques générales ou d'une pratique juridique établie relevant de différentes matières (droit civil, droit commercial, droit du travail) »[648]. Troisièmement, la responsabilité peut être accordée suite à un examen des circonstances factuelles (relations contractuelles entre les parties, attente raisonnable de la

638 La Cour de cassation a en effet estimé que, « en l'absence de fichier tel que défini à l'article 1er de la loi du 8 décembre 1992, celle-ci ne trouve pas à s'appliquer ».

639 Voy. le n° 113 de la présente chronique.

640 Pour une critique de cet arrêt, voy. C. DE TERWANGNE, « La difficile application de la législation de protection des données à caractère personnel », *J.T.*, 2017/38, p. 753 ; O. VANRECK, « Quand la Cour de cassation s'emmêle : du champ d'application de la loi du 8 décembre 1992 au droit d'accès », note sous Cass., 22 février 2017, *R.D.T.I.*, n° 66-67, pp. 165 et s.

641 La disposition mentionnée précise encore que « [l]orsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance ».

642 Le responsable de traitement y est défini comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ».

643 Le Groupe de travail Article 29 sur la protection des données est un organe européen indépendant traitant de questions relatives à la protection des données à caractère personnel et à la vie privée. Suite à l'entrée en vigueur du RGPD, il est remplacé par le Comité européen de la protection des données.

644 Groupe de travail Article 29 sur la protection des données, avis n° 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », WP 169, p. 10.

645 *Ibid.*

646 Art. 44, § 1er, de la loi du 24 juin 2013 relative aux sanctions administratives communales. Voy. C. const., 23 avril 2015, n° 44/2015, disponible sur www.juridat.be.

647 Art. 32*quater*/2, § 1er, du Code judiciaire. Voy. C. const., 5 octobre 2017, n° 108/2017, disponible sur www.juridat.be.

648 Groupe de travail Article 29 sur la protection des données, avis n° 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », WP 169, p. 11.

personne concernée, …)[649]. Ainsi, la cour de travail de Bruxelles a estimé que la banque faisant appel à un détective privé doit être considérée comme responsable du traitement (le traitement consistant en la réalisation d'un film et un rapport communiqué à la banque) tandis que le détective privé a agi en qualité de sous-traitant[650].

124. Responsabilité conjointe. La définition du responsable du traitement prévoit la possibilité que deux, voire plusieurs, responsables de traitement déterminent conjointement les finalités et moyens d'un traitement ce qui implique qu'ils soient désignés comme co-responsables de ce traitement. L'avocat général M. Yves Bot est revenu sur cette notion dans ses conclusions générales relatives à l'affaire *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*[651].

Dans cette affaire, une société spécialisée dans le domaine de l'éducation se plaignait d'une injonction prononcée à son encontre par l'autorité de protection des données compétente lui demandant de désactiver sa « page fan » hébergée sur le site de Facebook Ireland Ltd, en raison du fait que les visiteurs de cette page n'étaient pas informés de la collecte de leurs données par Facebook, par le biais de cookies de connexion.

Dans le cadre de l'examen des questions préjudicielles posées, l'avocat général a estimé que la collecte des données à caractère personnel des visiteurs, en vue d'établir des statistiques d'audience relative à cette page, constituait un traitement. Les responsables conjoints de ce traitement sont :

- Facebook Inc puisqu'elle « a mis au point le modèle économique conduisant à ce que la collecte de données à caractère personnel lors de la consultation de pages fan puis l'exploitation de ces données puissent permettre, d'une part, la diffusion de publicités personnalisées et, d'autre part, l'établissement de statistiques d'audience à destination des administrateurs de ces pages »[652] ;
- Facebook Ireland car elle « est désignée par Facebook Inc. comme étant chargée du traitement des données à caractère personnel au sein de l'Union »[653] ;
- la société spécialisée dans le domaine de l'éducation, administratrice de la page fan litigieuse, en ce qui concerne l'opération de collecte par Facebook des données à caractère personnel des visiteurs[654].

Dans son arrêt du 5 juin 2018, la Cour de justice a largement suivi les conclusions de l'avocat général et estimé que « l'article 2, sous d), de la directive 95/46/CE doit être interprété en ce sens que la notion de "responsable du traitement", au sens de cette disposition, englobe l'administrateur d'une page fan hébergée sur un réseau social »[655].

649 *Ibid.*, p. 12.
650 C. trav. Bruxelles, 18 mai 2015, R.G. n° 2014/AB/996, disponible sur www.juridat.be.
651 Conclusions de l'avocat général Y. Bot du 24 octobre 2017, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, ECLI:EU:C:2017:796, § 48.
652 *Ibid.*, point 48.
653 *Ibid.*, point 49.
654 *Ibid.*, point 50.
655 C.J.U.E., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16. Cet arrêt sera commenté dans la prochaine chronique.

4. Principes généraux (Noémie Gillard et Odile Vanreck)

125. Introduction. Comme rappelé dans l'arrêt *Peter Puškár*, « tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données énoncés à l'article 6 de ladite directive et, d'autre part, répondre à l'un des principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de cette même directive »[656]. Ces principes sont repris aux articles 4 et 5 de la loi du 8 décembre 1992.

126. Principe de loyauté. Le principe de loyauté, prévu à l'article 4, § 1er, 1°, de la loi du 8 décembre 1992[657], implique que le traitement des données à caractère personnel d'une personne soit effectué de manière transparente et, dès lors, que certaines informations soient fournies aux personnes concernées. À titre exemplatif[658], dans l'arrêt *Smaranda Bara*, la Cour de justice a rappelé que « l'exigence de traitement loyal des données personnelles (…) oblige une administration publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données »[659].

Ce principe de loyauté étant mis en œuvre par le biais de l'information à fournir aux personnes concernées, nous renvoyons à la partie consacrée au droit à l'information pour le développement des arrêts pertinents durant la période visée par la présente chronique[660].

127. Principe de finalité. Le principe de finalité est consacré à l'article 4, § 1er, 2°, de la loi du 8 décembre 1992[661]. En vertu de ce principe, les données doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités (…) »[662].

À ce sujet, la cour d'appel de Gand a estimé que « [l]'établissement de l'impôt des personnes physiques doit être vu comme une finalité déterminée, explicite et légitime au sens de l'article 4, § 1er, 2°, de la loi du 8 décembre 1992 »[663].

656 C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy*, aff. C-73/16, § 104.

657 Voy. art. 6.1.a de la directive 95/46/CE.

658 Le respect du principe de loyauté a également été évoqué par le demandeur dans les arrêts suivants : Liège (6e ch.), 13 octobre 2016, inédit ; Cass., 22 février 2017, R.G. no P.16.1110.F, disponible sur juridat.be.

659 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a. c. Președintele Casei Naționale de Asigurări de Sănătate e.a.*, aff. C-201/14, EU:C:2015:638, point 34.

660 Voy. nos 135 à 140.

661 Voy. art. 6.1.b de la directive 95/46.

662 Eu égard aux finalités, la directive 95/46 et la loi du 8 décembre 1992 prévoient également que les données à caractère personnel doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement » et « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement » (respectivement les articles 6.1.c et e de la directive 95/46 et 4, § 1er, 3° et 5°, de la loi du 8 décembre 1992).

663 Gand (5e ch.), 13 octobre 2015, *R.G.C.F.*, 2016/3, p. 236.

128. Principe de proportionnalité. Le principe de proportionnalité – qui s'applique tant au niveau du traitement dans son ensemble que des données à caractère personnel qu'il vise – est l'un des principes fondamentaux de la loi du 8 décembre 1992[664].

En vertu de ce principe, le traitement doit être proportionné au regard de la finalité légitime qu'il poursuit. Cela se traduit par l'exigence d'un examen de proportionnalité visant à déterminer si le traitement dont il est question est propre à réaliser l'objectif qu'il poursuit, et « s'il n'existe pas d'autres moyens moins contraignants » d'atteindre cet objectif[665].

C'est à un examen de ce type que s'est livrée la Cour constitutionnelle dans un arrêt concernant un traitement dans une banque de données policières, réalisé conformément à la loi du 18 mars 2014 relative à la gestion de l'information policière[666]. À cette occasion, la Cour a procédé à l'examen de plusieurs éléments du cadre légal instituant le traitement contesté, afin de déterminer si ce traitement, dans son ensemble, était proportionné. Elle a notamment examiné la présence de garanties portant sur la conservation, l'accès et l'effacement des données, ainsi que la pertinence et le caractère excessif, ou non, des données traitées[667].

Ce dernier élément – le caractère adéquat, pertinent et non excessif des données traitées – est un aspect central de l'examen de la proportionnalité d'un traitement[668]. L'arrêt *Tele2 Sverige* le démontre parfaitement[669].

Le principe de proportionnalité trouve également à s'exprimer dans l'article 4, § 1er, 5°, de la loi du 8 décembre 1992, prévoyant que les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ». Ainsi, dans un arrêt relatif à la conformité de la loi du 24 juin 2013 relative aux sanctions administratives communales avec l'article 22 de la Constitution, la durée du traitement a, parmi d'autres aspects, fait l'objet de discussions[670]. La réglementation en cause prévoyait que les communes conservent – et tiennent un registre contenant – les données des personnes ayant fait l'objet d'une sanction administrative pendant une durée de cinq ans. Malgré l'argumentation des parties requérantes selon laquelle cette durée dépassait le délai de prescription – qui était de deux ans –, la Cour a estimé que cette durée était justifiée, après avoir souligné qu'à l'issue de celle-ci les

664 Voy. C. de Terwangne et J.-M. Van Gyseghem, « Chapitre 3.2. Analyse détaillée de la loi protection des données et de son arrêté royal d'exécution », in C. de Terwangne (dir.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, pp. 67 et s.

665 C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy*, aff. C-73/16, point 113.

666 C. const., 14 juillet 2016, n° 108/2016, disponible sur www.juridat.be ; A. Bouvy, M. Borres, M. Solbreux, C. Nennen, P. Nihoul et J. Debry, « La Cour constitutionnelle – Chronique de jurisprudence 2016 », *R.B.D.C.*, 2017/3, p. 251.

667 C. const., 14 juillet 2016, n° 108/2016, B.79 et s., disponible sur www.juridat.be.

668 Art. 4, § 1er, 3°, de la loi du 8 décembre 1992.

669 C.J.U.E. (gr. ch.), 21 décembre 2016, *Tele2 Sverige AB c. Post- och telestyrelsen et Secretary of State for the Home Department c. Tom Watson e.a.*, aff. C-203/15 et C-698/15 ; à noter qu'un arrêt similaire a été rendu par la Cour constitutionnelle belge : voy. C. const., 11 juin 2015, n° 84/2015, disponible sur http://juridat.be. Voy. sur ce point, la section B1 de la présente chronique qui évoque de façon plus détaillée ces décisions.

670 Loi du 24 juin 2013 relative aux sanctions administratives communales, art. 25, § 1er, et 44 ; C. const., 23 avril 2015, n° 44/2015, disponible sur www.juridat.be.

données étaient soit effacées, soit anonymisées, et que le traitement en cause n'était pas prévu pour une durée illimitée[671].

129. Principe d'exactitude des données. En vertu de l'article 4, § 1er, 4°, de la loi du 8 décembre 1992[672], les données doivent être « exactes et si nécessaire, mises à jour ». Durant la période étudiée, la reconnaissance de la violation de ce principe d'exactitude a été réclamée dans une affaire opposant un client à sa banque[673]. Dans cette affaire, un client avait été enregistré au fichier des enregistrements non régis (ce qui lui avait causé un préjudice) suite à la communication d'informations erronées par la banque à la BNB. Le client/personne physique estimait que, par cette communication, la banque avait traité de manière inexacte et déloyale ses données. La cour d'appel de Liège avait estimé qu'il ne lui appartenait pas « de porter un jugement sur la gestion quotidienne de la banque et sur l'exécution de la convention des enregistrements non régis liant Belfius à la BNB ». La Cour de cassation, saisie de cette affaire, a estimé que cette motivation était régulière[674].

5. Licéité du traitement (Noémie Gillard)

130. Introduction. La condition de licéité du traitement, qui implique que le responsable du traitement doit pouvoir fonder son traitement sur une des hypothèses définies limitativement dans la législation, a fait l'objet de plusieurs décisions durant la période étudiée[675]. La Cour de justice a rappelé que « les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel audit article [7 de la directive 95/46/CE] ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article »[676].

131. Consentement – Portée territoriale. Un arrêt du 15 mars 2017 a donné à la Cour de justice l'occasion de se pencher sur la portée territoriale du consentement[677].

Cet arrêt concernait la demande, adressée par une société belge réalisant des annuaires publics (EDA) à des opérateurs de téléphonie néerlandais, de lui transmettre les données à caractère personnel de leurs abonnés situés sur le territoire des Pays-Bas, de manière à faire apparaître ces informations dans leurs annuaires. Elle se basait pour ce faire sur une disposition de droit néerlandais qui transposait la directive « service universel »[678]. Confrontée au refus des opérateurs,

671 C. const., 23 avril 2015, n° 44/2015, B.35.7, disponible sur www.juridat.be.

672 Voy. art. 6.1.d de la directive 95/46/CE.

673 Liège (6e ch.), 13 octobre 2016, inédit.

674 Cass., 22 février 2017, R.G. n° P.16.1110.F, disponible sur www.juridat.be. Sur cet arrêt, voy. les nos 113 et 122 dans la présente chronique. Voy. également C. de Terwangne, « La difficile application de la législation de protection des données à caractère personnel », *J.T.*, 2017/38, p. 753 ; O. Vanreck, « Quand la Cour de cassation s'emmêle : du champ d'application de la loi du 8 décembre 1992 au droit d'accès », note sous Cass., 22 février 2017, *R.D.T.I.*, 2017, n° 66-67, pp. 165 et s.

675 Pour ce qui concerne une application de cette exigence lors de l'utilisation de cookies, voy. le n° 157.

676 C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14, § 57 ; dans le même sens, C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy*, aff. C-73/16, point 105.

677 C.J.U.E., 15 mars 2017, *Tele2 (Netherlands) BV e.a. c. Autoriteit Consument en Markt (ACM)*, aff. C-536/15.

678 Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive « service universel »).

la société EDA avait saisi l'Autorité néerlandaise des consommateurs et des marchés (ACM), qui lui avait donné raison. C'est dans la continuité du recours des opérateurs contre cette décision que deux questions préjudicielles ont été posées à la Cour de justice.

Au travers de l'une de ces questions, il était demandé à la Cour si le transfert des données à caractère personnel d'un abonné vers une entreprise dont les services consistaient en la fourniture d'annuaires publics, dans un autre État membre que celui dans lequel l'abonné résidait, devait faire l'objet d'un consentement distinct et spécifique de cet abonné[679].

C'est une réponse négative qui a été apportée à cette question. Selon la Cour, dès lors qu'un abonné a donné son consentement à un opérateur pour que ses données apparaissent dans un annuaire public, son droit à la protection des données à caractère personnel ne peut être violé par la transmission de ces données à une entreprise tierce sollicitant les informations visées à l'article 25, § 2, de la directive « service universel », même si celle-ci fournit ses services sur le territoire d'un autre État membre[680].

132. Respect d'une obligation légale. Un traitement de données à caractère personnel peut être nécessaire au respect d'une obligation légale qui s'impose au responsable de traitement[681]. La disposition qui établit une telle obligation doit cependant répondre à certaines exigences destinées à assurer la prévisibilité du traitement constituant une ingérence dans la vie privée des personnes dont les données sont ainsi traitées. Dans un arrêt de 2016, la Cour constitutionnelle a rappelé qu'une loi prévoyant un traitement de données à caractère personnel devait être claire et précise[682]. La Cour a souligné dans cet arrêt que (i) la nature et la qualité des données susceptibles d'être traitées, ainsi que les circonstances dans lesquelles elles peuvent l'être[683] et (ii) les catégories de personnes dont les données peuvent faire l'objet d'un traitement devaient être clairement et précisément déterminées[684].

133. Mission d'intérêt public ou exercice de l'autorité publique. En vertu de l'article 5, e), de la loi du 8 décembre 1992, le traitement de données à caractère personnel est autorisé lorsque le responsable de traitement est chargé d'une mission d'intérêt public, ou relevant de l'exercice de l'autorité publique, nécessitant la mise en œuvre de ce traitement.

La Cour de justice a considéré que la tenue, par une autorité publique, d'un registre contenant des données fournies par des sociétés sur la base d'obligations légales, ainsi que l'organisation de la consultation de ce registre par les personnes intéressées et l'octroi de copies relevaient de ce « motif de légitimation »[685]. La Cour a souligné que ce traitement, prévu par la directive 68/151/

679 C.J.U.E., 15 mars 2017, *Tele2 (Netherlands) BV e.a. c. Autoriteit Consument en Markt (ACM)*, aff. C-536/15, point 31.
680 *Ibid.*, points 36-41.
681 Art. 5, c), de la loi du 8 décembre 1992.
682 C. const., 14 juillet 2016, n° 108/2016, B.11.2-3, disponible sur www.juridat.be.
683 *Ibid.*, B.46 et s.
684 *Ibid.*, B.28 et s.
685 C.J.U.E., 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, aff. C-398/15, point 42.

CEE[686], contribuait à la protection des intérêts des tiers dans le cadre de leurs relations avec les sociétés par actions et sociétés à responsabilité limitée[687].

Il a également été jugé par la Cour de justice que l'établissement d'une liste, reprenant les noms de personnes physiques occupant fictivement des fonctions de direction au sein d'une ou plusieurs personnes morales, ne violait pas nécessairement la directive 95/46/CE, même si les personnes concernées n'avaient pas consenti au traitement de leurs données à caractère personnel[688]. La Cour a en effet estimé que la mise en place d'une telle liste était susceptible de relever de l'article 7, e), de la directive 95/46/CE, étant donné que l'objectif poursuivi était de permettre la perception de l'impôt et la lutte contre la fraude fiscale[689].

Dans le même ordre d'idées, la cour d'appel de Gand a jugé que la consultation du répertoire matricule des véhicules, dans la mesure où cette consultation était nécessaire à l'établissement de l'impôt des personnes physiques, ne constituait pas une violation de la loi du 8 décembre 1992. L'établissement de l'impôt relève ainsi, selon la Cour, de l'intérêt général et est couvert par l'hypothèse décrite à l'article 5, e), de cette loi, qui correspond à l'article 7, e), de la directive[690].

134. Intérêt légitime poursuivi par le responsable du traitement. Dans un arrêt récent[691], la Cour de justice a rappelé les trois conditions cumulatives, prévues par l'article 7, f), de la directive 95/46/CE, devant être rencontrées pour qu'un traitement relevant de ce cas de figure soit licite, à savoir : (i) la poursuite d'un intérêt légitime, (ii) la nécessité du traitement pour la réalisation de l'intérêt légitime poursuivi, et (iii) la condition que les droits et libertés fondamentaux de la personne concernée ne prévalent pas[692]. Tout d'abord, la Cour a jugé que l'intérêt d'une personne à obtenir des données à caractère personnel appartenant à un tiers qui avait porté atteinte à sa propriété, en vue de l'assigner en justice pour obtenir réparation, constituait bien un « intérêt légitime »[693]. Ensuite, la juridiction européenne s'est brièvement penchée sur la condition de nécessité[694], avant d'apporter des précisions intéressantes quant aux éléments à prendre en compte dans le cadre de la pondération des intérêts en présence. Elle a ainsi relevé qu'il pouvait être pertinent d'avoir égard au fait que les données en question se trouvaient dans des sources déjà accessibles au public, ainsi qu'à la circonstance que la personne concernée était mineure[695].

Par ailleurs, l'arrêt rendu par la Cour de justice de l'UE dans l'affaire *Patrick Breyer* a également été l'occasion pour la Cour de traiter de l'article 7, f), de la directive, cette fois-ci en lien avec une légis-

686 Directive 68/151/CEE du Conseil du 9 mars 1968 tendant à coordonner, pour les rendre équivalentes, les garanties qui sont exigées, dans les États membres, des sociétés au sens de l'article 58, deuxième alinéa, du traité, pour protéger les intérêts tant des associés que des tiers, *J.O.C.E.* L 65 de 1968, p. 8.

687 C.J.U.E., 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, aff. C-398/15, point 49.

688 C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy*, aff. C-73/1.

689 *Ibid.*, point 110.

690 Gand (5e ch.), 13 octobre 2015, *R.G.C.F.*, 2016/3, p. 236.

691 C.J.U.E., 4 mai 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA « Rīgas satiksme »*, aff. C-13/16.

692 *Ibid.*, point 28.

693 *Ibid.*, point 29.

694 *Ibid.*, point 30.

695 *Ibid.*, points 30-33.

lation allemande contestée[696]. Cette législation nationale permettait à un fournisseur de services de média en ligne de passer outre le consentement de l'utilisateur du service et de collecter et utiliser ses données à caractère personnel, uniquement dans la mesure où la collecte et l'utilisation de ces données étaient nécessaires à la facturation de l'utilisation concrète du service. Il était par contre exclu par la réglementation en question que l'objectif de fonctionnement général du média en ligne permette de justifier l'utilisation des données après une session de consultation du média.

Dans ce contexte, la Cour a estimé que la disposition allemande n'était pas conforme avec l'économie de l'article 7, f), étant donné qu'elle réduisait de manière excessive la portée de la notion d'« intérêt légitime » établie par le texte européen. La disposition litigieuse aboutissait en effet à interdire définitivement, et sans permettre ni la pondération des intérêts en présence ni la prise en compte des circonstances spécifiques d'une situation concrète, la possibilité de traiter certaines catégories de données à caractère personnel[697].

6. Droits de la personne concernée (Alejandra Michel)

135. Importance de l'information de la personne concernée et de son droit d'accès comme préalable à l'exercice de l'ensemble de ses droits. Que ce soit en vertu des articles 10 et 11 de la directive 95/46/CE ou de l'article 9 de la loi du 8 décembre 1992, la personne dont les données à caractère personnel font l'objet d'un traitement a le droit d'obtenir, de la part du responsable du traitement, une série d'informations dont celle relative à l'existence de droits d'accès et de rectification. La jurisprudence, tant au niveau européen qu'en droit interne, souligne la primordialité de cette information pour la personne concernée constituant le préalable nécessaire à la mise en œuvre de l'ensemble de ses droits (accès, rectification et opposition)[698]. Par ailleurs, l'exercice, par la personne concernée, de son droit d'accès – corollaire du droit d'être informée – est également élevé au rang d'indispensable pour la mise en œuvre d'autres droits[699]. Comme l'a déclaré la Cour de justice, « ce droit d'accès est nécessaire, notamment, pour permettre à la personne concernée d'obtenir, le cas échéant, de la part du responsable du traitement, la rectification, l'effacement ou le verrouillage [des] données […] »[700]. Par ailleurs, la cour d'appel de Liège a eu l'occasion d'indiquer que ce droit d'accès, accessoire du droit à la protection de la vie privée, confère, à la personne concernée, « un droit de regard sur l'utilisation qui est faite de ses données à caractère personnel traitées sous la forme d'un fichier en vérifiant qui a accédé à ces informations et dans quel but »[701].

136. Extension des exemptions à l'information de la personne concernée. Suite à l'arrêt de la Cour constitutionnelle rendu en date du 3 avril 2014 déclarant que l'application automatique

696 C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14.

697 *Ibid.*, points 55 et s.

698 Voy. notamment C.J.U.E. (3e ch.), 1er octobre 2015, *Smaranda Bara*, aff. C-201/14, point 33 ; C.J.U.E. (2e ch.), 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, aff. C-434/16, point 48 ; C. trav. Liège (6e ch.), 6 février 2015, *J.T.T.*, 2015/29, p. 299. En effet, il est primordial que la personne concernée soit informée de ses droits d'accès et de rectification pour pouvoir effectivement en réclamer l'application. Sans information, la personne concernée est privée de la possibilité d'exercer ses droits.

699 C.J.U.E. (2e ch.), 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, aff. C-434/16, points 56 et 57.

700 *Ibid.*, point 57.

701 Liège (6e ch. corr.), 13 octobre 2016, R.G. n° 2015/IC/9, www.juridat.be. Voy. également Cass. (2e ch), 22 février 2017, *J.T.*, 2017/38, p. 751, note C. de Terwangne.

du devoir d'information de la personne concernée aux détectives privés agréés violait les principes d'égalité et de non-discrimination[702], un recours en annulation des articles 3, §§ 3-6 (catégories de personnes ou d'institutions exonérées de l'obligation d'informer la personne concernée), et 9 (information de la personne concernée) de la loi du 8 décembre 1992 a été introduit. La Cour constitutionnelle s'est prononcée le 25 février 2016[703]. Les requérants estimaient que ces dispositions opéraient une différence de traitement discriminatoire entre les catégories de personnes et d'institutions listées à l'article 3 de la loi et les organismes publics légalement chargés de se prononcer sur les manquements déontologiques des professions réglementées. Bien que l'analyse opérée dans l'arrêt du 3 avril 2014 visait des détectives privés agréés, la Cour constitutionnelle étend ses précédents enseignements à l'organisme professionnel pour le compte duquel travaillent les détectives privés[704]. Par conséquent, en attendant la modification légale de la liste des exemptions, la Cour estime que les organismes publics ayant pour mission légale de rechercher les manquements déontologiques d'une profession réglementée et les détectives privés autorisés à agir pour ces organismes ne doivent pas être soumis à l'obligation d'information figurant à l'article 9 de la loi[705].

137. Information de la personne concernée et détective privé. Dans un arrêt du 6 février 2015 antérieur à la jurisprudence évoquée sous le point 2, la cour d'appel de Liège s'est prononcée sur le droit d'information de la personne concernée ayant fait l'objet d'une enquête réalisée par un détective privé[706]. Elle estime que le rapport du détective privé doit respecter les dispositions de la loi du 8 décembre 1992. Ainsi, selon le paragraphe 2 de l'article 9, la personne concernée ayant fait l'objet d'une collecte indirecte doit notamment être informée de l'existence d'un droit d'accès et d'un droit de rectification[707]. Dans l'hypothèse d'un traitement de données à caractère personnel réalisé par un détective privé, la cour d'appel estime que l'information de la personne concernée peut se faire lors de la rédaction du rapport mais en tout état de cause avant l'utilisation du rapport en justice afin qu'elle puisse adéquatement exercer ses droits et éventuellement s'opposer au traitement de données[708].

138. Information de la personne concernée et utilisation de caméras de vidéosurveillance. Dans un arrêt du 25 mars 2017, la cour d'appel de Gand a analysé le respect du devoir d'information à l'égard de la personne concernée dont les données n'ont pas été obtenues directement auprès d'elle, prévue dans le paragraphe 2 de l'article 9 de la loi du 8 décembre 1992[709] dans

[702] Pour le détail de cet arrêt, nous renvoyons à la précédente chronique, *R.D.T.I.*, 2015, n° 59-60, pp. 71-72.

[703] C. const., 25 février 2016, arrêt n° 28/2016.

[704] *Ibid.*, B.10.

[705] *Ibid.*, B.11.

[706] C. trav. Liège (6e ch.), 6 février 2015, *J.T.T.*, 2015/29, p. 298. Pour un commentaire de cette décision, voy. K. Rosier, « Détectives privés et vie privée : mener l'enquête, mais pas en toute discrétion », in *Recueil de jurisprudence : responsabilité – assurances – accidents du travail*, Limal, Anthemis, 2015, pp. 35-55.

[707] C. trav. Liège (6e ch.), 6 février 2015, *J.T.T.*, 2015/29, p. 299. Dans le même sens concernant également un rapport de détective privé, voy. Trib. trav. Bruxelles (5e ch.), 15 mai 2015, R.G. n° 2014/AB/996, www.juridat.be, pp. 12 et 13.

[708] C. trav. Liège (6e ch.), 6 février 2015, *J.T.T.*, 2015/29, p. 299. La cour se ralliant en l'espèce à la thèse de D. Mougenot selon lequel informer la personne concernée au moment de la rédaction du rapport permet de ne pas gâcher l'effet de surprise essentiel à l'enquête du détective privé.

[709] Rappelons qu'en vertu de cette disposition, le responsable du traitement est tenu de fournir toute une série d'informations à la personne concernée : identité du responsable du traitement, finalités du traitement, droit de s'opposer au traitement à des fins de marketing direct, existence des droits d'accès et de rectification, etc.

le contexte de l'utilisation de caméras de vidéosurveillance[710]. La Cour a suivi le raisonnement des défendeurs selon lequel, par l'apposition d'un pictogramme contenant diverses informations (vidéosurveillance en tant que finalité du traitement, loi applicable et société responsable), les personnes concernées ont été adéquatement informées des circonstances dans lesquelles les caméras de vidéosurveillance sont placées et utilisées[711]. La cour d'appel de Gand mentionne dès lors que l'apposition d'un tel pictogramme permet à la personne concernée d'exercer, si elle le désire, ses droits dans le cadre de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance[712].

139. Information de la personne concernée et transfert de données entre administrations publiques. Avec l'arrêt *Smaranda Bara*, la Cour de justice s'est penchée sur l'information de la personne concernée lors du transfert des données la concernant d'une administration publique à une autre[713]. Les requérants estimaient que le transfert de leurs données fiscales d'une administration à une autre n'avait pas respecté la directive 95/46/CE en ce que lesdites données avaient été réutilisées pour d'autres finalités, donnant ainsi lieu à un traitement ultérieur incompatible avec la finalité initiale et réalisé sans en avoir été informés. Précisons que la loi roumaine impose à l'Agence nationale d'administration fiscale de transmettre à la Caisse nationale de sécurité sociale « les données nécessaires à l'établissement de la qualité d'assuré »[714]. Toutefois, pour ce faire, seules les données d'identification des personnes sont pertinentes, et non celles relatives aux revenus, puisque la Cour note que même des citoyens sans revenus imposables se voient attribuer la qualité d'assuré[715]. Aux yeux de la Cour de justice, une telle base légale ne doit alors pas s'entendre comme une information préalable libérant le responsable du traitement de son devoir d'informer la personne concernée au sens de l'article 10 de la directive 95/46/CE[716]. Ainsi, l'obligation de traiter les données loyalement impose d'informer la personne concernée lors de la transmission des données la concernant d'une administration publique à l'autre « en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données »[717].

140. Banque et information de la personne concernée. Dans l'arrêt du 13 octobre 2016 susmentionné, la banque n'ayant jamais transmis au client une copie de l'ensemble des contrats signés avec la banque, ce dernier a décidé d'intenter sa responsabilité pour infraction à l'article 39, 5°, de la loi du 8 décembre 1992. Malgré le fait que la cour d'appel de Liège ait estimé que les contrats bancaires ne constituaient pas un fichier faisant l'objet d'un traitement au sens de la loi du 8 décembre 1992, elle a tout de même relevé une obligation d'information à charge de la banque quant aux documents bancaires en ces termes : « la communication de ces documents, dont au demeurant la partie civile devait nécessairement disposer d'une copie, relève de l'obligation d'information de la banque et ne peut rentrer dans le champ pénal de la loi du 8 décembre

710 Gand, 25 mars 2017, R.G. n° 2015/NT/185, www.juridat.be.
711 *Ibid.*
712 *Ibid.*
713 C.J.U.E. (3e ch.), 1er octobre 2015, *Smaranda Bara*, aff. C-201/14.
714 *Ibid.*, point 11.
715 *Ibid.*, points 16 et 37.
716 *Ibid.*, point 38. Précisons que la Cour va tenir un raisonnement analogue pour l'article 11 de la directive 95/46/CE.
717 *Ibid.*, point 34.

1992 »[718]. Soulignons néanmoins un manque de clarté quant à cette « obligation d'information de la banque » : relève-t-elle d'une loi particulière du secteur bancaire ou de la loi du 8 décembre 1992[719] ?

141. Banque et droit d'accès. Dans ce même arrêt, la cour d'appel de Liège a curieusement réduit la portée du droit d'accès du client aux informations relatives à ses opérations bancaires suite à une notification selon laquelle la banque mettait fin à l'utilisation de sa carte de crédit. En l'espèce, le client souhaitait se voir communiquer les opérations réalisées avec une carte de crédit dont il n'avait finalement jamais été le détenteur. La cour d'appel a ici retenu que la communication réalisée par l'agent bancaire permettait au client par déduction de disposer des informations nécessaires. Cette position sera ultérieurement confirmée par la Cour de cassation par un arrêt du 22 février 2017[720]. Alors qu'elle avait par le passé indiqué qu'à sa demande, la personne concernée avait le droit de se voir effectivement communiquer les informations relatives aux données la concernant sans tenir compte du fait qu'elle les détenait déjà par ailleurs[721], la Cour de cassation a confirmé l'arrêt de la cour d'appel de Liège en estimant que, vu que le client avait été informé du fait qu'il n'avait jamais été détenteur de la carte de crédit, il lui était possible de « déduire qu'aucune opération réalisée au moyen de cette carte de crédit n'avait été enregistrée sur son compte »[722].

142. Examen et droits d'accès, de rectification et d'effacement. Avec l'arrêt *Peter Nowak c. Data Protection Commissioner*, la Cour de justice s'est penchée sur l'étendue des droits d'accès et de rectification de la personne ayant passé un examen[723]. Le requérant s'était vu refuser, par le commissaire à la protection des données irlandais, l'accès à la copie corrigée d'un examen de comptabilité qu'il avait présenté au motif qu'il ne s'agissait pas d'une donnée à caractère personnel. Après avoir considéré que les réponses d'un candidat à un examen ainsi que les annotations du correcteur constituaient bel et bien des données à caractère personnel au sens de la directive 95/46/CE, la Cour de justice a explicité les conséquences d'une telle qualification.

Précisons d'abord que la Cour est d'avis que l'ouverture des droits d'accès et de rectification ne doit aucunement être de nature à modifier cette qualification en donnée à caractère personnel[724]. En effet, ce n'est pas parce que l'exercice des droits d'accès et de rectification reçoit une connotation particulière dans le contexte d'examens qu'il faudrait pour autant estimer que les réponses fournies par un candidat n'ont pas vocation à constituer des données à caractère personnel.

Ensuite, la Cour considère que la possibilité pour la personne concernée d'exercer ses droits d'accès et de rectification présente bien un intérêt dans l'hypothèse d'un examen que cette dernière a

718 Liège (6e ch. corr.), 13 octobre 2016, R.G. n° 2015/IC/9, www.juridat.be. Voy. également concernant cette décision, *infra*, n° 148.

719 La Cour de cassation, dans le cadre du pourvoi introduit contre l'arrêt, n'a pas été saisie de cette question (Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, p. 751, note C. de Terwangne).

720 Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, p. 751, note C. de Terwangne.

721 C. de Terwangne, « La difficile application de la législation de protection des données à caractère personnel », obs. sous Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, pp. 753-754.

722 Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, pp. 751 et 752.

723 C.J.U.E. (2e ch.), 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, aff. C-434/16.

724 C.J.U.E. (2e ch.), 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, aff. C-434/16, point 46.

présenté[725]. S'il est indéniable que le droit de rectification ne pourrait être utilisé par le candidat pour corriger des réponses erronées au vu de l'appréciation du caractère exact et complet par rapport à la finalité du traitement[726], il n'en demeure pas moins que l'on pourrait considérer que les réponses du candidat et les annotations de l'examinateur soient inexactes ou incomplètes dans la mesure où, par exemple, le candidat est confronté à la perte d'une partie de ses réponses, à l'inversion de ses réponses avec celle d'un autre candidat ou encore à une justification insuffisante de sa note par les annotations de l'examinateur[727]. Il en découle, aux yeux de la Cour de justice, que les droits d'accès et de rectification s'étendent, non pas aux questions d'examen en tant que telles, mais aux réponses du candidat ainsi qu'aux annotations du correcteur[728].

La Cour souligne, par ailleurs, que le candidat est également en droit d'adresser une requête au responsable du traitement en vue de l'effacement des données à caractère personnel le concernant dans l'examen, c'est-à-dire de ses réponses ainsi que des annotations de l'examinateur, dès lors que les finalités du traitement initial ou ultérieur ont été réalisées[729]. En ce qui concerne les réponses d'un candidat à un examen ainsi que les annotations du correcteur, la Cour mentionne que « leur conservation dans une forme permettant l'identification du candidat ne paraît, *a priori*, plus nécessaire une fois que la procédure d'examen est définitivement close et ne peut plus faire l'objet de recours, de telle sorte que ces réponses et annotations ont perdu toute valeur probante »[730].

143. Droit à l'oubli. Dans deux arrêts – le premier en degré d'appel, le second en cassation –, la jurisprudence belge rappelle que le droit à l'oubli[731] est une composante du droit au respect de la vie privée garanti tant en droit interne par l'article 22 de la Constitution, en droit européen par l'article 8 de la Convention européenne des droits de l'homme qu'en droit international en vertu de l'article 17 du Pacte international relatif aux droits civils et politiques[732]. Pour le détail de ces deux arrêts concernant des archives de médias en ligne, nous renvoyons le lecteur au titre IV « Médias, liberté d'expression et nouvelles technologies »[733].

144. Droit à l'effacement. Sans que cela ne soit explicitement mentionné par la Cour de justice, c'est bien de droit à l'effacement dont il est question dans l'arrêt *Manni*[734].

725 *Ibid.*, point 51.

726 Sur ce point, la Cour mentionne que la finalité du traitement dans le cadre d'un examen a pour but d'« évaluer le niveau de connaissance et de compétence de ce candidat à la date de l'examen » et que les erreurs participent justement à l'évaluation du niveau atteint par le candidat. Voy. *ibid.*, point 53.

727 *Ibid.*, points 52 à 54.

728 *Ibid.*, points 54 et 58.

729 *Ibid.*, point 55.

730 *Ibid.*, point 55.

731 Pour rappel, le droit à l'oubli judiciaire est une prérogative offerte à une personne s'étant retrouvée à un moment donné au centre de l'actualité judiciaire de se faire « oublier » et d'ainsi s'opposer, sous réserve du respect de certaines conditions, à une nouvelle divulgation de son « passé judiciaire ». Il se distingue du droit à l'oubli numérique permettant à un internaute de conserver la maitrise des données à caractère personnel le concernant diffusées sur internet en réclamant leur effacement. Sur ce point, voy. Cass. (1re ch.), 29 avril 2016, *J.T.*, 2016, pp. 612 et 614.

732 Liège (20e ch.), 4 février 2016, *A&M*, 2016/5-6, p. 464 ; Cass. (1re ch.), 29 avril 2016, *J.T.*, 2016, p. 617.

733 Voy. les nos 264 à 268.

734 C.J.U.E. (2e ch.), 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, aff. C-398/15.

Les parties en litige débattaient la question de savoir si, à l'issue de l'expiration d'un certain délai suivant la cessation des activités d'une entreprise et à la demande de la personne concernée, il existait une obligation dans le chef de l'autorité chargée de la tenue d'un registre contenant des informations répondant à une exigence de publicité, d'effacer ou d'anonymiser les données à caractère personnel y figurant, ou encore d'en limiter la publicité[735]. La personne concernée, Monsieur Manni, faisait valoir que la présence, dans ce registre, de l'information selon laquelle sa première affaire avait fait faillite plus de dix ans auparavant portait préjudice à son activité actuelle.

La Cour a examiné la question sous l'angle du droit d'opposition de la personne concernée[736] et a rappelé la nécessité d'opérer une pondération des intérêts de la personne concernée avec la finalité poursuivie par le traitement[737]. Elle a relevé, à cet égard, que la réglementation sur laquelle reposait le traitement litigieux avait pour objectif de préserver les intérêts des tiers dans leurs rapports d'affaires avec les entreprises concernées[738]. Soulignant que ces tiers pouvaient toujours justifier d'un intérêt à accéder à certaines informations même après dissolution de la société[739], ainsi que la variété des délais de prescription prévus dans les différents États membres[740], la Cour a fini par conclure qu'il ne pouvait être garanti aux personnes concernées que leurs données soient effacées, anonymisées ou leur accès limité dans des conditions telles que celles de l'espèce[741].

7. Flux transfrontières (Manon Knockaert)

145. Flux transfrontières de données et pouvoir des autorités de contrôle nationales. La période étudiée est marquée par l'arrêt de la Cour de justice opposant Maximilian Schrems au géant américain du réseau social Facebook[742]. M. Schrems, ressortissant européen, s'était opposé à l'envoi de ses données à caractère personnel vers les serveurs de Facebook Inc. localisés aux États-Unis. Considérant que, malgré la décision rendue par la Commission européenne[743], un niveau de protection adéquat de ses données à caractère personnel n'était pas assuré outre-Atlantique, M. Schrems avait décidé de saisir l'autorité de contrôle irlandaise.

735 *Ibid.*, point 44.

736 Art. 14 de la directive 95/46.

737 C.J.U.E. (2e ch.), 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, aff. C-398/15, point 47.

738 *Ibid.*, points 49-50.

739 *Ibid.*, points 53 et 60.

740 *Ibid.*, point 54.

741 *Ibid.*, point 56.

742 C.J.U.E., 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, aff. C-362/14. Sur cet arrêt, voy. K. Rosier, « L'arrêt *Schrems* de la C.J.U.E. : un coup d'arrêt au transfert de données à caractère personnel vers les États-Unis », *Bulletin juridique et social*, 2016, p. 6 ; C. De Terwangne et C. Gayrel, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse : les impacts de l'arrêt *Schrems* », *Cahiers de droit européen*, 2017, p. 35.

743 Décision 2000/520 de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, *J.O.C.E.* L 215, p. 7. Par cette décision, la Commission européenne valide le système mis en place aux États-Unis, permettant ainsi le transfert des données depuis l'Europe vers les entreprises américaines. Sur ce point, voy. *infra*, le n° 146.

Saisie sur questions préjudicielles posées par la High Court irlandaise, la Cour de justice a ainsi été amenée à se prononcer tant sur la validité de cette contestation que sur les pouvoirs de l'autorité de contrôle face à une décision d'adéquation de la Commission européenne. Après avoir insisté sur l'importance des autorités indépendantes[744] – véritables garantes de l'effectivité du respect de la protection des personnes à l'égard du traitement des données à caractère personnel[745] –, la Cour analyse leurs prérogatives à la lumière de l'article 28 de la directive 95/46/CE. Elle rappelle que l'autorité nationale de contrôle est en charge de vérifier que les transferts de données à caractère personnel depuis l'État membre dont elle relève respectent toutes les exigences de la réglementation[746] et elle estime dans la foulée que cette compétence doit être maintenue nonobstant une décision d'adéquation de la Commission européenne[747].

En effet, la conclusion inverse déforcerait l'effectivité de la protection des droits fondamentaux des individus[748]. Néanmoins, la Cour précise qu'elle est seule compétente pour annuler un acte de l'Union[749]. Sur la base de ces éléments, la Cour conclut que l'autorité de contrôle peut rejeter la demande de la personne concernée si elle est d'avis que les éléments qu'elle avance sont dépourvus de fondement. La personne concernée conserve par ailleurs la possibilité d'être entendue par un juge qui doit sursoir à statuer et saisir la Cour de justice par renvoi préjudiciel en appréciation de validité.

En revanche, s'il subsiste des doutes quant à la conformité de la décision d'adéquation au regard du droit de l'Union, l'autorité nationale doit saisir les juridictions nationales afin que celles-ci puissent procéder à un renvoi préjudiciel devant la Cour de justice[750].

146. Flux transfrontières de données et *Safe Harbor*. Dans la même affaire, la décision *Safe Harbor* a été remise en cause. Par cette décision, la Commission européenne reconnait que les principes visés à l'annexe première ainsi que la FAQ y relative permettent de donner le feu vert aux transferts de données à caractère personnel vers les entreprises qui, sur une base purement volontaire d'auto-certification, adhèrent aux principes de la « sphère de sécurité ».

Cette décision s'inscrit dans le cadre de l'article 25, paragraphe 2, de la directive 95/46/CE qui nécessite une appréciation du niveau de protection offert par un pays se trouvant en dehors de l'Union européenne au regard du droit et des pratiques dudit pays : ce pays tiers doit offrir aux données des citoyens européens un niveau de protection adéquat. Aux yeux de la Cour, la protection offerte doit être substantiellement équivalente au régime européen[751]. De surcroît, elle impose un contrôle strict de cette exigence laissant peu de pouvoir d'appréciation à la Commission européenne[752].

744 Par le passé, la Cour de justice avait souligné l'importance d'une indépendance réelle et effective pour les autorités de contrôle ; voy. C.J.U.E. (gr. ch.), 16 octobre 2012, *Commission c. Autriche*, aff. C-614/10 et C.J.U.E. (gr. ch.), 9 mars 2010, *Commission c. Allemagne*, aff. C-518/07.

745 C.J.U.E., 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, aff. C-362/14, point 41.

746 *Ibid.*, point 44.

747 *Ibid.*, points 54 à 57.

748 *Ibid.*, point 58.

749 *Ibid.*, point 52.

750 *Ibid.*, points 64 et 65.

751 *Ibid.*, point 73.

752 *Ibid.*, point 78.

Le système du *Safe Harbor* imaginé par la Commission européenne est condamné pour plusieurs motifs.

Premièrement, si la Cour ne rejette en principe pas un système d'auto-certification, elle requiert que celui-ci soit accompagné de mécanismes efficaces de détection et de contrôle afin d'identifier et de sanctionner les règles de protection des droits au respect de la vie privée et à la protection des données à caractère personnel[753].

Deuxièmement, dans la décision critiquée de la Commission européenne, cette dernière se borne à un simple constat d'adéquation, sans démontrer à suffisance les fondements qui sous-tendent ce constat[754]. De plus, la Cour de justice condamne la prévalence – pouvant figurer dans un texte de nature législative, administrative ou une décision jurisprudentielle – des motifs de sécurité nationale, d'intérêts publics et du respect des lois en vigueur aux États-Unis sur la protection des données[755]. À l'estime de la Cour, le caractère général de cette dérogation et de cette ingérence vide de leur substance les règles de protection énoncées en amont[756]. La Cour relève qu'une réglementation permettant un accès généralisé et une conservation par les autorités américaines du contenu de toutes les communications électroniques des personnes dont les données sont transférées ne peut être considérée comme limitée au strict nécessaire[757]. En outre, les personnes concernées sont dépourvues des voies de recours administratives ou judiciaires leur permettant d'exercer leurs droits d'accès, de rectification et de suppression[758].

L'équivalence substantielle du niveau de protection des données à caractère personnel paraît incompatible avec une réglementation n'entourant pas de règles claires et précises l'ingérence afin de la limiter au strict nécessaire[759]. Par conséquent, la Cour pointe que la Commission européenne ne motive pas dûment la compatibilité de la décision susmentionnée avec la protection des libertés et des droits fondamentaux[760].

Par ailleurs, la décision 2000/520 de la Commission limite les pouvoirs des autorités nationales de contrôle en écartant la possibilité pour celles-ci de prendre des mesures visant à assurer le respect des principes entourant le transfert de données à caractère personnel vers un pays tiers. La Cour, se basant sur une interprétation stricte du texte de la directive qui prévoit que les autorités de protection connaissent – en toute indépendance – de toutes demandes relatives à la protection de ses données à caractère personnel par une personne concernée, constate un dépassement de ses pouvoirs par la Commission européenne[761]. La décision d'adéquation est donc déclarée invalide, bloquant ainsi les transferts de données à caractère personnel de l'Union européenne vers les États-Unis[762].

753 *Ibid.*, point 81.
754 *Ibid.*, point 83.
755 *Ibid.*, points 84 et 85.
756 *Ibid.*, point 87.
757 *Ibid.*, points 88-94.
758 *Ibid.*, point 95.
759 *Ibid.*, point 94.
760 *Ibid.*, point 96.
761 *Ibid.*, points 101-104.
762 *Ibid.*, point 106.

Dans un contexte de globalisation des échanges de données, cette jurisprudence a fait craindre des répercussions importantes pour les acteurs économiques. Rapidement, la Commission a entamé des négociations avec les États-Unis pour négocier un nouvel accord permettant aux données à caractère personnel d'à nouveau traverser l'océan. Ces pourparlers ont donné naissance au *Privacy Shield*[763]. Suite à cette décision, une société à but non lucratif irlandaise, militant pour la protection des libertés sur internet, a saisi la Cour de justice[764]. Toutefois, la Cour déclare le recours irrecevable pour défaut d'intérêt à agir[765]. En l'absence de statuts lui attribuant une habilitation à agir en justice au nom et pour le compte de ses membres, la Cour relève que le droit de l'Union ne permet pas une *actio popularis* fondée sur l'intérêt général[766]. De plus, le recours intenté par la requérante en son nom propre est également déclaré irrecevable. En effet, en sa qualité de personne morale, elle n'entre pas dans le champ d'application matériel de la réglementation[767]. Elle ne peut par ailleurs pas invoquer sa qualité de responsable du traitement des données à caractère personnel de ses membres puisque le « *Privacy Shield* » ne restreint pas ses droits et ne lui impose par ailleurs aucune obligation additionnelle[768].

8. Responsabilité et sanctions (Manon Knockaert)

147. Diffusion sur internet de données à caractère personnel et responsabilité civile. L'affaire en cause concernait la diffusion, suite au dépôt d'une pétition sur le site internet du Parlement européen, de données à caractère personnel relatives à la santé d'un ancien fonctionnaire du Conseil de l'Union européenne[769]. En l'espèce, le requérant avait présenté au Parlement, par le biais d'un formulaire en ligne, une pétition relative au soutien accordé aux membres handicapés de sa famille, aux difficultés auxquelles sont confrontés les fonctionnaires européens victimes de problèmes de santé pendant leur carrière et au mauvais traitement de son dossier par le Conseil[770]. Cette pétition fut rejetée mais s'en est suivie la publication d'une communication sur le site internet du Parlement. Ladite communication décrivait sommairement la pétition et mentionnait notamment le nom du requérant ayant adressé la pétition, le fait qu'il souffrait d'une maladie grave et le handicap de son fils. Par conséquent, le requérant souhaitait engager la responsabilité aquilienne de l'Union du fait de ses agents[771]. Il incombe à la Cour de vérifier le triptyque faute-dommage-lien causal. Pour que la faute dans le chef du Parlement européen soit retenue, il faut démontrer une violation suffisamment caractérisée d'une règle de droit de l'Union. Le débat s'est alors porté sur le respect du règlement n° 45/2001/CE relatif à la protec-

763 Décision d'exécution 2016/1250/UE relative à l'adéquation de la protection assurée par le bouclier de protection des données EU-États-Unis.

764 Trib. (ord.), 22 novembre 2017, *Digital Rights Ireland Ltd*, aff. T-670/16.

765 *Ibid.*, point 54.

766 *Ibid.*, points 47-50. Relevons toutefois que le nouveau règlement général sur la protection des données (RGPD) permet aux États membres de prévoir pour tout organisme, organisation ou association le droit d'introduire une plainte auprès de l'autorité nationale de contrôle compétente, et ce indépendamment de tout mandat confié par une personne concernée (art. 80 et considérant 140 de la réglementation).

767 *Ibid.*, points 24 et 26.

768 *Ibid.*, points 33-36.

769 Trib. (6e ch.), 3 décembre 2015, *CN c. Parlement européen*, aff. T-343/13.

770 *Ibid.*, point 1.

771 En effet, l'article 340, alinéa 2, du traité sur le fonctionnement de l'Union européenne (TFUE) dispose que : « En matière de responsabilité non contractuelle, l'Union doit réparer conformément aux principes généraux communs aux droits des États membres, les dommages causés par ses institutions ou par ses agents dans l'exercice de leurs fonctions ».

tion 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[772] lors de la diffusion sur internet des données et lors de la demande de suppression de ses données par la partie requérante.

Toutefois, la Cour ne retient aucune faute dans le chef du Parlement.

En effet, avant de procéder au dépôt en ligne de sa pétition, le site du Parlement recommande à la personne concernée de prendre connaissance de l'aide en ligne indiquant que certaines informations – dont le nom – sont disponibles sur internet et qu'il revient au pétitionnaire d'explicitement demander que ses informations ne soient pas divulguées publiquement. Par ailleurs, au moment du dépôt de sa pétition, la personne est amenée à remplir un formulaire pour marquer son accord avec le traitement public de sa demande et l'inscription de son nom dans le registre public sur internet[773]. Par conséquent, puisqu'en cochant les cases, la personne a répondu par l'affirmative aux questions du formulaire, la Cour estime que le requérant a valablement consenti de manière explicite et informée au traitement de ses données sensibles[774].

En outre, la Cour est d'avis que le Parlement, bien que non tenu de répondre positivement à la demande d'effacement[775], a réagi promptement à cette demande et a agi dans un délai raisonnable[776]. En l'absence de faute, la responsabilité du Parlement ne peut être engagée. Néanmoins, la Cour estime que, malgré le fait que le recours doive être rejeté en raison de l'absence de faute, il est opportun d'examiner les autres arguments soulevés par la partie requérante[777]. Dès lors, la Cour poursuit son analyse et se penche sur l'existence du préjudice certain dont la démonstration incombe à celui qui s'en prévaut. De la sorte, la Cour énonce les principes applicables lorsqu'une faute est établie. La Cour interprète cette condition comme nécessitant un préjudice imminent et prévisible avec une certitude suffisante même s'il ne peut encore être déterminé avec précision. *A contrario*, la Cour rejette un préjudice purement hypothétique[778]. La Cour admet les frais de conseils juridiques au titre de préjudice matériel mais elle estime qu'il ne peut être attribué au Parlement puisque l'engagement de tels frais relève du simple choix du requérant[779].

148. Articulation entre une sanction disciplinaire et la réglementation relative à la protection des données à caractère personnel. Au cours de la période étudiée, la Cour de cassation a eu l'occasion de se prononcer sur la compatibilité de la juxtaposition d'une sanction disciplinaire avec une sanction pénale pour violation de la loi du 8 décembre 1992 et du principe général du droit *non bis in idem*[780]. La Cour suit le raisonnement des juges d'appel en déclarant que cette

772 Règlement n° 45/2001/CE du Parlement européen et du Conseil du 18 décembre 2000 relatif 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.*, 8 décembre 2001, pp. 1-22.

773 Trib. (6e ch.), 3 décembre 2015, *CN c. Parlement européen*, aff. T-343/13, points 64 et 65.

774 *Ibid.*, point 74.

775 En effet, l'article 16 du règlement n° 45/2001/CE octroie un droit à l'effacement pour la personne concernée qu'en présence d'un traitement illicite.

776 Trib. (6e ch.), 3 décembre 2015, *CN c. Parlement européen*, aff. T-343/13, points 90 et 100.

777 *Ibid.*, point 110.

778 *Ibid.*, point 118.

779 Trib. U.E. (6e ch.), 3 décembre 2015, *CN c. Parlement européen*, aff. T-343/13, points 123 et 124.

780 Cass. (2e ch.), 14 octobre 2015, *Rev. dr. pén. entr.*, 2016/2, p. 169.

action disciplinaire ne pouvait s'apparenter à une sanction pénale. Partant, une sanction disciplinaire ne fait pas obstacle à l'application de l'article 39 de la loi relative à la vie privée punissant d'une amende le responsable du traitement, son représentant en Belgique, son préposé ou le mandataire qui violerait les dispositions de la loi du 8 décembre 1992[781].

149. Pouvoir de sanction et compétence territoriale des autorités de contrôle nationales. En vertu de l'article 28 de la directive 95/46/CE, les autorités de contrôle sont, indépendamment du droit applicable au traitement des données à caractère personnel, compétentes pour surveiller l'application de la législation sur le territoire de l'État membre dont elles relèvent. En l'espèce, il s'agissait d'un site internet d'annonces de biens immobiliers situés en Hongrie par une société immatriculée en Slovaquie. Certains annonceurs demandaient le retrait de leurs données à caractère personnel du site internet après la période d'essai d'un mois. En l'occurrence, en dépit du fait que le droit applicable coïncidait avec le ressort territorial de l'autorité de contrôle dont la compétence était remise en cause[782], la Cour a été invitée à se prononcer sur la question de la marge de manœuvre dont dispose l'autorité de contrôle souhaitant exercer ses prérogatives lorsque le droit applicable au traitement est celui d'un autre État membre. La Cour rappelle que chaque autorité de contrôle peut être saisie d'une plainte par toute personne[783]. C'est donc à bon droit que les annonceurs détenant des biens en Hongrie décident de saisir l'autorité de contrôle hongroise. La Cour, sensible à la souveraineté territoriale, au principe de légalité et à la notion d'État de droit[784], précise cependant que, dans une hypothèse où le droit applicable au traitement est celui d'un autre État membre que celui auquel appartient l'autorité de contrôle, cette autorité ne peut exercer la totalité des pouvoirs dont elle est normalement investie[785]. La Cour en conclut que, bien que l'autorité de contrôle saisie d'une plainte conserve ses pouvoirs d'investigation, cela n'entraine pas la possibilité d'imposer des sanctions à un responsable de traitement non établi sur son territoire[786]. Seul l'État membre dont la compétence est déterminée par le droit applicable au traitement se voit doté d'une telle prérogative[787]. La Cour insiste dès lors sur la nécessaire coopération entre autorités de contrôle de l'Union européenne[788].

150. Sanction pénale et dol spécial. La cour d'appel de Liège[789] a eu l'occasion de préciser que la violation des dispositions légales relatives à la vie privée et à la protection des données à caractère personnel, déclenchant l'application de l'article 39, 1°, de la loi du 8 décembre 1992 dans son

781 *Ibid.*, p. 170. Sur ce point, voy. titre 6, chapitre II de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

782 La Cour de justice estime que le traitement rentre bien dans le cadre des activités d'un responsable de traitement sur le territoire de l'État membre dont dépend l'autorité de contrôle en cause. Sur les notions d'« établissement du responsable de traitement », voy. *supra*, le n° 123.

783 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o.*, aff. C-230/14, point 39.

784 *Ibid.*, point 56.

785 *Ibid.*, point 55.

786 *Ibid.*, point 57.

787 *Ibid.*, point 60.

788 *Ibid.*, point 52.

789 Liège (6e ch. corr.), 13 octobre 2016, R.G. n° 2015/IC/9, www.juridat.be. La Cour de cassation a confirmé la décision : Cass. (2e ch.), 22 février 2017, *J.T.*, 2017/38, p. 752.

volet pénal, implique nécessairement la démonstration d'un dol spécial[790]. En l'espèce, la cour considère que, si une mauvaise gestion documentaire ayant abouti au fichage de la personne pourrait éventuellement entraîner la responsabilité civile de la banque, il n'en va pas de même pour la responsabilité pénale puisque la faute commise ne rencontre pas l'élément moral de l'infraction[791].

151. Injonction sous astreinte. Dans l'affaire concernant l'utilisation du cookie Datr par Facebook[792] pour collecter des données à caractère personnel de personnes non membres du réseau social[793], la Commission de la protection de la vie privée belge a demandé en référé au président du tribunal de condamner Facebook Inc, Facebook Ireland Limited[794] et la SPRL Facebook Belgium[795], sous peine d'une astreinte d'un montant de 250.000 euros par jour de non-exécution, à arrêter ses pratiques consistant à suivre les habitudes de navigation des résidents belges non inscrits.

Le président du tribunal insiste sur le caractère massif et manifeste de la violation, touchant un nombre très important d'individus au regard de l'abondante présence de sites internet dotés des plug-ins sociaux de Facebook[796]. Il rappelle que la loi du 8 décembre 1992 est applicable et qu'elle permet de sanctionner le responsable de traitement, son représentant en Belgique, son préposé ou encore son mandataire[797]. Par conséquent, la mesure demandée par la Commission peut non seulement être imposée à la société américaine mais également à Facebook Ireland et à la société belge Facebook Belgium. En outre, eu égard au chiffre d'affaires et aux bénéfices de Facebook, le président estime que le montant de l'astreinte permet d'ajouter un caractère dissuasif à la sanction sans pour autant paraître disproportionnée[798]. Récemment, dans un jugement rendu le 16 février 2018[799], le tribunal de première instance de Bruxelles confirme la mesure ordonnée par le président du tribunal et exige en outre la suppression des données à caractère personnel collectées illicitement[800].

B. Questions spéciales concernant les communications électroniques (Alejandra Michel)

1. Les communications électroniques et la rétention des données

152. Annulation de la loi belge transposant la directive 2006/24/CE sur la conservation des données de trafic. Suite à l'invalidation de la directive 2006/24/CE relative à la conservation des données de trafic[801], un recours en annulation de la loi du 30 juillet 2013 transposant en droit

790 Liège (6e ch. corr.), 13 octobre 2016, R.G. n° 2015/IC/9, www.juridat.be, p. 7. Sur ce point, voy. titre 6, chapitre II de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

791 *Ibid.*, p. 7.

792 Civ. Bruxelles (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, p. 91.

793 Voy. les nos 155-160.

794 Facebook Ireland Limited offre les services du réseau social aux utilisateurs européens.

795 La SPRL Facebook Belgium est une société créée afin d'assurer la gestion des relations avec les autorités et le lobbying.

796 Civ. Bruxelles (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, p. 109.

797 *Ibid.*, p. 109. Sur ce point, voy. titre 6, chapitre II de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *op. cit.*

798 *Ibid.*, pp. 109-110.

799 Civ. Bruxelles (24e ch.), 16 février 2018, R.G. n° 2016/153/A, inédit. Ce jugement sera analysé lors de la prochaine chronique.

800 Sur ce point, voy. le n° 160.

801 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

belge cette même directive et modifiant la loi belge du 13 juin 2005 relative aux communications électroniques a été introduit auprès de la Cour constitutionnelle[802]. L'article 126 de la loi du 13 juin 2005, après modification, prévoyait la conservation des données de trafic, de localisation et d'identification des utilisateurs, des services de communications électroniques et des équipements terminaux utilisés générées ou traitées par les fournisseurs de services de communications accessibles au public ou de réseaux publics de communications, à des fins de lutte contre la criminalité, durant douze mois à partir de la date de la communication.

Les requérants déploraient que cette disposition traite identiquement, d'une part, les utilisateurs devant respecter un éventuel secret professionnel et ceux n'étant pas soumis à une telle obligation et, d'autre part, les utilisateurs objet de mesures d'enquête ou de poursuite pénale et ceux pour lesquels il n'existe aucun indice d'infractions pénales[803]. La Cour constitutionnelle va alors rappeler les enseignements de l'arrêt *Digital Rights*[804] rendu le 8 avril 2014 par la Cour de justice et invalidant la directive 2006/24/CE, selon lesquels l'obligation de conservation des données de trafic, de localisation et d'identification – données intrinsèquement liées à la vie privée et aux communications de l'internaute – ainsi que l'accès à ces données par les autorités compétentes constituent une ingérence particulièrement grave dans le droit fondamental de l'individu au respect de sa vie privée[805]. La Cour constitutionnelle reprend ensuite l'analyse de la Cour de justice déclarant que l'ingérence en cause n'était pas limitée au strict nécessaire.

Premièrement, puisque la loi attaquée devant la Cour constitutionnelle prévoyait, à l'instar de la directive 2006/24/CE invalidée par la Cour de justice, la conservation généralisée de toutes les données de trafic de toutes personnes par tous moyens de communication électronique sans distinguer selon les objectifs de lutte contre la criminalité, la Cour constitutionnelle en déduit qu'elle s'applique, d'une part, à des personnes dont il n'existe aucun indice pouvant laisser croire qu'elles adoptent un comportement en lien avec les infractions que le législateur souhaite poursuivre et, d'autre part, sans prévoir des exceptions pour les personnes soumises à une obligation de secret professionnel[806].

Deuxièmement, la Cour relève l'absence de lien entre les données conservées et une éventuelle menace pour la sécurité publique ainsi que l'absence de limitations temporelle, géographique ou des personnes visées par la conservation des données de trafic et l'absence de condition à remplir pour les autorités compétentes souhaitant accéder à ces données[807].

Troisièmement et enfin, la Cour constitutionnelle pointe du doigt que la disposition légale discutée ne prévoie aucune distinction de durée de conservation des données en fonction des

de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, 13 avril 2006. Cette directive harmonisait les législations internes des États membres quant à la durée de conservation des données de trafic par les fournisseurs de réseaux publics de communications ou de services de communications accessibles au public à des fins de lutte contre la criminalité. Sur ce point, voy. précédente chronique, *R.D.T.I.*, 2015, n° 59-60, pp. 84-85.

802 C. const., 11 juin 2015, n° 84/2015.

803 *Ibid.*, B.2.2.

804 Pour le détail de cet arrêt, nous renvoyons le lecteur à la précédente chronique, *R.D.T.I.*, 2015, n° 59-60, pp. 84-85. Voy. en particulier les points 54, 57, 58, 59, 63, 64 et 65 de l'arrêt *Digital Rights*.

805 C. const., 11 juin 2015, n° 84/2015, B.6 et B.9.

806 *Ibid.*, B.10.1.

807 *Ibid.*, B.10.2 et B.10.3.

personnes concernées ou en fonction de l'utilité que les données possèdent pour la lutte contre la criminalité[808].

La Cour constitutionnelle conclut alors, sur la base des mêmes arguments que ceux développés par la Cour de justice dans l'arrêt *Digital Rights*, à l'annulation totale de la loi du 30 juillet 2013[809].

153. Conséquences de l'arrêt de la Cour constitutionnelle du 11 juin 2015 sur la jurisprudence des juridictions belges. À ce stade, nous nous devons de préciser que cet arrêt d'annulation de la loi du 30 juillet 2013 dans son ensemble rendu par la Cour constitutionnelle a eu des conséquences sur la jurisprudence des juridictions belges.

Dans un arrêt rendu le 20 juillet 2015, la chambre des mises en accusation de la cour d'appel de Gand a fait écho à l'annulation, par la Cour constitutionnelle, de la loi belge sur la conservation des données de trafic[810]. En l'espèce, le dossier pénal avait notamment été constitué grâce aux données transférées aux autorités judiciaires par des fournisseurs de réseaux publics de communications ou de services de communications accessibles au public. En effet, ces derniers conservaient les données de trafic en vertu de l'obligation légale imposée par l'article 5 de la loi du 30 juillet 2013 modifiant la loi du 13 juin 2005 sur les communications électroniques. Après avoir rappelé les enseignements de l'arrêt d'annulation de la Cour constitutionnelle, la chambre des mises en accusation va préciser que sa portée se limite aux métadonnées, c'est-à-dire « aux données individuelles qui peuvent être liées à un accusé spécifique dans le cadre d'une enquête judiciaire »[811]. Elle estime par ailleurs que lesdites informations ont été réclamées, sur la base d'un cadre juridique et d'une décision motivée, par un juge d'instruction indépendant. Par ailleurs, en vertu des articles 122 et 123 de la loi sur les communications électroniques, la conservation des données de localisation et d'appel par les opérateurs est déjà nécessaire à la fourniture de leurs services, à la gestion de leur réseau de communication électronique, à la facturation de leurs services aux clients ainsi que pour la détection de fraude éventuelle[812]. Par conséquent, la chambre des mises en accusation en déduit que ces données sont légalement collectées par les opérateurs. À son estime, même s'il était considéré que les données avaient été irrégulièrement obtenues vu que la Cour constitutionnelle a jugé que leur conservation par les opérateurs et les fournisseurs était fondée sur une disposition légale inconstitutionnelle, elle ne considère pas que les données disponibles dans le dossier pénal ne pourraient pas être utilisées ou qu'il faudrait conclure à leur nullité[813].

De son côté, le tribunal correctionnel de Gand s'est également prononcé sur les conséquences à conférer à l'arrêt d'annulation de la loi du 30 juillet 2013 rendu par la Cour constitutionnelle[814]. Tout d'abord, le tribunal confronte les versions de l'article 126 de la loi sur les communications électroniques avant et après la modification introduite par l'article 5 de la loi du 30 juillet 2013 qui va ainsi prévoir la conservation généralisée et indifférenciée des données de communica-

808 *Ibid.*, B.10.4.
809 *Ibid.*, B.11 et B.12.
810 Gand (ch. mis. acc.), 20 juillet 2015, *T. strafr.*, 2016/2, p. 189.
811 *Ibid.* (traduction libre).
812 *Ibid.*
813 *Ibid.*
814 Corr. Bruges (16e ch.), 29 juin 2015, *T.G.R.*, 2015, p. 358.

tions électroniques par les fournisseurs de réseaux publics de communications ou de services de communications accessibles au public[815]. Ensuite, le tribunal précise que, vu qu'en l'espèce il a à se prononcer sur une période d'emprisonnement ayant débuté avant l'introduction et l'entrée en vigueur d'une telle modification, il est ici question de l'ancienne version de l'article 126 de la loi du 13 juin 2005 qui n'a jamais fait l'objet d'un recours en annulation[816]. Aux yeux du tribunal, l'arrêt de la Cour constitutionnelle du 11 juin 2015 est uniquement susceptible d'être sujet à discussions pour les actions d'enquête menées, sur la base de l'article 126 de la loi sur les communications électroniques telle que modifiée par l'article 5 de la loi du 30 juillet 2013, après l'entrée en vigueur de la loi du 30 juillet 2013, c'est-à-dire à partir du 2 septembre 2013[817].

154. Non-compatibilité au droit de l'Union d'une conservation généralisée et indifférenciée des données de communications électroniques. Dans un arrêt *Tele2 Sverige AB*, la Cour de justice s'est prononcée, en grande chambre, sur les conséquences de l'arrêt *Digital Rights*[818] pour la conservation des données de trafic et de localisation[819]. Au centre de cette affaire, un conflit d'interprétation de la portée à conférer à l'invalidation de la directive sur la conservation des données relatives aux communications électroniques entre un fournisseur de services de communications électroniques et une autorité nationale de surveillance des postes et des télécommunications (ci-après, « PTS »). Vu l'invalidation de la directive 2006/24/CE par la Cour de justice, Tele2 Sverige avait averti PTS qu'il cesserait pour l'avenir toute conservation des données portant sur les communications électroniques de ses clients[820]. Estimant que Tele2 Sverige ne respectait pas l'obligation légale qui lui était imposée en vertu d'une législation nationale, PTS lui a ordonné de conserver les données de trafic et de localisation de ses clients à des fins de lutte contre la criminalité[821]. Dans le cadre du recours contre l'injonction introduit par Tele2 Sverige, la juridiction de renvoi questionne la Cour de justice afin de savoir si, au vu de l'invalidation de la directive 2006/24/CE, l'article 15, paragraphe 1er, de la directive 2002/58/CE s'oppose à la conservation généralisée et indifférenciée, à des fins de lutte contre la criminalité, de l'ensemble des données de localisation et de trafic de tous les clients et pour tous les moyens de communications électroniques[822].

Avant toute chose, la Cour de justice constate que cette législation nationale entre dans le champ d'application de la directive 2002/58/CE, entre autres parce que cette dernière vise les traitements de données à caractère personnel dans des hypothèses de fournitures de services de communications électroniques[823]. Par ailleurs, la Cour de justice rappelle que la directive 2002/58/CE prône l'effacement ou l'anonymisation des données de trafic et de localisation lorsqu'elles ne sont plus de nature à permettre la transmission d'une communication électronique mais qu'en son article 15, paragraphe 1er, elle permet aux États membres de limiter cette obligation, notamment en imposant, à des fins de lutte contre les infractions pénales, la conservation des données pour

815 *Ibid.*, pp. 358 à 360.
816 *Ibid.*, p. 360.
817 *Ibid.*
818 Sur l'arrêt *Digital Rights* invalidant la directive 2006/24/CE, voy. précédente chronique, *R.D.T.I.*, 2015, nº 59-60, pp. 84-85.
819 C.J.U.E. (gr. ch.), 21 décembre 2016, *Tele2 Sverige AB*, aff. C-203/15 et C-698/15.
820 *Ibid.*, point 44.
821 *Ibid.*, point 47.
822 *Ibid.*, points 50 et 62.
823 *Ibid.*, points 64 à 81.

une période déterminée[824]. La Cour insiste toutefois sur les conditions entourant cette possibilité de dérogation : d'une part, l'énumération des objectifs permettant de la justifier est exhaustive et, d'autre part, les mesures dérogeant au principe de confidentialité des communications électroniques doivent être nécessaires, appropriées et proportionnées dans une société démocratique et doivent être analysées à la lumière des droits fondamentaux au respect de la vie privée, à la protection des données à caractère personnel et à la liberté d'expression[825]. Concernant la législation nationale en cause, la Cour souligne qu'elle prévoit la conservation généralisée, indifférenciée, systématique et continue, par les fournisseurs de services de communications électroniques, de toutes les données de localisation et de trafic de l'ensemble de leurs clients pour tous les moyens de communication électronique, sans prévoir ni exceptions ni limitations temporelle, géographique ou personnelle[826]. Un tel spectre de données à conserver permet « de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées » et crée ainsi une ingérence grave dans le droit fondamental au respect de la vie privée[827]. La Cour de justice conclut à l'incompatibilité de la législation nationale visée avec le droit de l'Union[828]. Précisons toutefois qu'aux yeux de la Cour, les États membres ont la possibilité de prendre des mesures préventives imposant la conservation ciblée des données de communications électroniques, à des fins de lutte contre la criminalité, à la condition qu'elles soient limitées au strict nécessaire tant quant aux personnes visées, aux catégories de données concernées, aux moyens de communication utilisés qu'à la durée de leur conservation[829].

2. L'usage de cookies

155. Introduction : usage de cookies à des fins de traçage comportemental. Dans une affaire en référé opposant Facebook[830] à la Commission de la protection de la vie privée belge, le président du tribunal de première instance de Bruxelles a ordonné au géant du réseau social de ne plus faire usage de cookies Datr et de plug-ins sociaux[831] pour suivre les habitudes de navi-

824 Pour information, l'article 15, paragraphe 1er, de la directive 2002/58/CE prévoit que « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État –, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, *les États membres peuvent*, entre autres, *adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* ».

825 C.J.U.E. (gr. ch.), 21 décembre 2016, *Tele2 Sverige AB*, aff. C-203/15 et C-698/15, points 90 à 95.

826 *Ibid.*, points 97, 105 et 106.

827 *Ibid.*, points 99 et 100.

828 *Ibid.*, point 112.

829 *Ibid.*, point 108.

830 L'affaire impliquait tant Facebook Inc, Facebook Ireland Limited et Facebook Belgium.

831 Rappelons brièvement qu'un cookie est un fichier texte envoyé au navigateur par le serveur web et conservé par le navigateur pour une utilisation future. Ainsi, ce fichier sera envoyé au serveur web initial à chaque nouvelle demande d'accès du navigateur. Précisons que les cookies Datr utilisés par Facebook rendent possible une identification unique du navigateur d'un internaute pour une durée de deux ans, y compris ceux qui ne possèdent pas de compte Facebook. Les plug-ins sociaux sont quant à eux des éléments introduits directement sur un site web afin d'offrir aux utilisateurs des possibilités d'interaction avec un réseau social. Pour une explication complète du fonctionnement des cookies et des plug-ins sociaux, voy. Civ. Bruxelles (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, pp. 92 à 94.

gation des non-utilisateurs belges de Facebook, c'est-à-dire des personnes ne possédant pas un compte sur ce réseau social[832]. Précisons qu'en degré d'appel, la cour a réformé cette ordonnance rendue le 9 novembre 2015 s'estimant incompétente en ce qui concerne Facebook Inc. ainsi que Facebook Ireland Limited : elle a ainsi considéré que sa compétence se limitait à la filiale belge du réseau social[833]. La cour d'appel va encore estimer qu'à défaut d'urgence la demande de la C.P.V.P. est sans fondement : la pratique de traçage des personnes non affiliées au réseau social ayant débuté en 2012, il n'existe donc aucune urgence à l'estime de la cour[834].

156. Cookies, notion de données à caractère personnel et traitement de données. Dans cette ordonnance du 9 novembre 2015, le président va d'abord considérer que, contrairement à la position défendue par Facebook, les cookies Datr – qui contiennent un « *unique identifier* » – enregistrés sur le navigateur de l'internaute constituent bel et bien des données à caractère personnel au sens de l'article 1er de la loi du 8 décembre 1992 puisqu'ils permettent l'identification unique du navigateur web d'un internaute déterminé[835]. Par ailleurs, le président souligne que Facebook reçoit également l'adresse IP de l'internaute qui rend alors possible, de manière directe ou indirecte, son identification[836]. Ensuite, étant donné que l'enregistrement et la réception automatisée des adresses IP et des cookies Datr répondent à la définition du traitement, le président précise que les dispositions de la loi du 8 décembre 1992, concernant entre autres le consentement de la personne concernée, doivent être respectées[837].

157. Cookies, consentement de la personne concernée et traitement illicite. L'ordonnance en référé du président du tribunal de première instance de Bruxelles dans l'affaire des cookies Facebook va également traiter la question du consentement de l'internaute non inscrit à l'usage, par le réseau social, de cookies Datr. Ainsi, le président va indiquer qu'il est indéniable que les personnes ne possédant pas un compte Facebook n'ont pas pu consentir à l'utilisation de cookies Datr pour traiter leurs données à caractère personnel puisqu'elles n'ont à aucun moment accepté les conditions générales d'utilisation du réseau social[838]. Par ailleurs, la mise en place d'une bannière présumant l'acceptation des cookies n'a pas convaincu le président de l'existence d'un consentement éclairé[839]. En effet, puisque les cookies Datr s'enregistrent notamment dès que l'internaute non inscrit visite les hyperliens intégrés à une page d'information sur les cookies ou lorsqu'il quitte un plug-in social en cliquant sur « annuler », cet enregistrement a lieu alors que, soit la personne continue strictement à s'informer sans pour autant profiter des services Facebook, soit se refuse justement à utiliser de tels services en quittant le plug-in social[840]. Dès lors,

832 Civ. Bruxelles (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, p. 91. À l'origine du conflit, se trouve notamment un rapport du ICRI de la KU Leuven constatant que Facebook réalisait également des traitements de données à caractère personnel de personnes non inscrites à l'aide des cookies et des plug-ins sociaux. Voy. *ibid.*, p. 96.

833 Bruxelles (réf., 18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016, no 62, p. 111 (somm.), note G. Dejemeppe. Voy. également *supra*, les nos 114 et 115.

834 *Ibid.*

835 *Ibid.*, pp. 103 et 104.

836 *Ibid.*, p. 104. L'ordonnance cite sur ce point la position de la Cour de justice qui a déjà, à maintes reprises, souligné que les adresses IP entraient dans la notion de données à caractère personnel.

837 *Ibid.*

838 *Ibid.*

839 *Ibid.*, p. 105. Cette bannière indique : « Les cookies nous permettent de fournir, protéger et améliorer les services de Facebook. En continuant à utiliser notre site, vous acceptez notre Politique d'utilisation des cookies ».

840 *Ibid.*

alors que les personnes inscrites sur Facebook sont présumées avoir à tout le moins donné un consentement implicite mais indubitable pour l'enregistrement et l'accès ultérieur aux cookies, il n'en va pas de même pour un internaute visitant ponctuellement une page du réseau social sans être titulaire d'un compte[841]. Puisque Facebook enregistre les données à caractère personnel des internautes non affiliés, en amont de leur parfaite information, pour des finalités non déterminées, non explicites et illégitimes, l'ordonnance précise qu'il réalise alors un traitement illicite[842].

158. Stockage et consultation des cookies déjà enregistrés sur le terminal de l'utilisateur non inscrit et article 129 de la loi du 13 juin 2005. Quant au stockage et à la consultation des cookies préalablement enregistrés, le président du tribunal considère que ces actes sont également réalisés sans le consentement éclairé et indubitable des internautes ne possédant pas un compte Facebook[843]. Rappelons à cet égard que l'article 129 de la loi relative aux communications électroniques exige que le responsable du traitement obtienne le consentement de l'utilisateur tant pour le stockage que pour l'accès aux informations déjà stockées sur son terminal. En outre, le président estime que, quoi qu'il en soit, les non-membres de Facebook ne sont pas des « utilisateurs » au regard de l'article 129 de la loi du 13 juin 2005 « qui demanderai[en]t explicitement un service Facebook chaque fois qu'il visite un site web de tiers sur lequel un plug-in social a été implémenté »[844].

159. Cookies, respect d'une obligation légale de Facebook en tant que responsable du traitement et intérêt légitime du responsable du traitement. Dans cette même affaire, le président va par ailleurs considérer que Facebook, en tant que responsable du traitement, ne peut s'appuyer sur aucun des trois fondements juridiques tirés de l'article 5 de la loi du 8 décembre 1992 dont il entendait se prévaloir[845].

Après avoir fermement rejeté le premier, à savoir le fondement du traitement sur le consentement indubitable de la personne concernée, le président va analyser l'argument de Facebook selon lequel son traitement serait justifié par une obligation légale. En l'occurrence, Facebook arguait que l'utilisation du cookie se justifiait au regard de l'article 16, paragraphe 4, de la loi du 8 décembre 1992 qui impose de prendre les mesures techniques et organisationnelles adéquates afin d'assurer la protection des données à caractère personnel contre tout problème de sécurité et d'intégrité. Le président va considérer que cette obligation ne s'impose au responsable du traitement qu'à partir du moment où la condition d'un motif justifiant le traitement est rencontrée[846]. Aussi, sous peine de vider de son sens la loi du 8 décembre 1992, il constate que « les obligations

841 *Ibid.*, p. 106.

842 *Ibid.*

843 *Ibid.*, p. 105.

844 *Ibid.*

845 *Ibid.*, pp. 106 à 108. Indiquons que le président a rapidement rejeté les fondements relatifs à la nécessité du traitement pour l'exécution d'un contrat ou de la phase précontractuelle, à la sauvegarde d'un intérêt vital de l'internaute non affilié à Facebook et à l'accomplissement d'une mission d'intérêt public.

846 *Ibid.*, p. 107 : « Il y a en effet lieu de vérifier d'abord si un motif d'admissibilité de l'article 5 peut être invoqué. Dans la négative, le traitement des données à caractère personnel n'est pas autorisé. Or, ce n'est que lorsque le traitement des données à caractère personnel est autorisé que naît l'obligation de prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel ».

légales au sens de l'article 5, c, de la loi relative à la protection de la vie privée ne désignent donc naturellement que des obligations stipulées dans d'autres lois que la loi relative à la protection de la vie privée elle-même […]»[847]. Pour le président, en décider autrement reviendrait à créer dans le cas d'espèce une situation aberrante validant le traitement des données d'internautes non inscrits, sans leur consentement, pour justifier la sécurisation des données à caractère personnel des membres du réseau social[848].

Quant au troisième fondement dont Facebook entendait se prévaloir, à savoir l'intérêt légitime de Facebook à sécuriser ses services, le président l'écarte également au motif que l'utilisation et la consultation des cookies Datr servant, notamment, à pallier les tentatives d'accès frauduleux ne se justifient pas à l'égard des non-membres du réseau social qui n'ont précisément pas à accéder aux services offerts par ledit réseau social[849]. Par ailleurs, outre l'existence de pratiques moins invasives pour sécuriser la plateforme, il est relevé qu'il ne fait nul doute que les pirates informatiques qui souhaitent diriger une attaque à l'encontre de Facebook n'éprouveront aucune difficulté à recourir à un logiciel bloquant le cookie Datr[850].

160. Récent jugement au fond. Dans un tout récent jugement rendu au fond le 16 février 2018, le tribunal de première instance de Bruxelles a donné raison à la C.P.V.P. dans le litige l'opposant au célèbre réseau social[851]. Le Tribunal, après s'être déclaré compétent tant concernant Facebook Belgium que Facebook Inc. et Facebook Ireland Limited lorsqu'ils suivent les habitudes de navigation d'internautes en Belgique, a relevé une information insuffisante des internautes quant à la collecte et aux traitements de leurs données à caractère personnel[852]. Par ailleurs, le tribunal est d'avis que le réseau social n'est pas en mesure de se prévaloir d'un consentement valable des internautes pour les traitements réalisés[853]. Par conséquent, Facebook se voit enjoindre, sous peine d'une astreinte de 250.000 euros par jour de retard, d'une part, de stopper ses activités consistant à suivre et à enregistrer les habitudes de navigation des internautes en Belgique aussi longtemps qu'elle ne respectera pas la loi du 8 décembre 1992 et, d'autre part, de supprimer les données à caractère personnel collectées en non-conformité avec la législation belge[854].

C. 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)

161. Contexte de la jurisprudence analysée. La présente analyse propose plus particulièrement un aperçu de la jurisprudence dans le contexte d'une prise de connaissance et utilisation par un employeur de données de communications électroniques, d'informations sur un support de stockage, ou par le biais de la vidéosurveillance ou de la géolocalisation, et ce notamment à la lumière de décisions de principes rendues par la Cour de cassation en matière de contrôle et d'utilisation de données de communication.

847 *Ibid.*
848 *Ibid.*
849 *Ibid.*, p. 108.
850 *Ibid.*
851 Civ. Bruxelles (24e ch.), 16 février 2018, R.G. no 2016/153/A, inédit.
852 *Ibid.*
853 *Ibid.* La décision n'est toutefois pas définitive, Facebook ayant annoncé entendre interjeter appel de la décision.
854 *Ibid.* Nous renvoyons le lecteur à prochaine chronique dans laquelle cette décision sera analysée plus en détail.

1. Les communications électroniques

162. Cadre légal. Nous devons constater, comme dans les chroniques précédentes[855], qu'il est difficile de dégager des tendances claires dans l'interprétation et l'application du cadre légal applicable. Face à des situations impliquant des technologies similaires, les juridictions ne mobilisent d'ailleurs pas forcément les mêmes textes légaux. Il est question des règles issues de la protection du droit au respect de la vie privée[856] et de la protection des données[857] et de dispositions particulières relatives aux communications électroniques[858]. Le texte du compromis qu'est celui de la CCT n° 81[859] reste également toujours d'actualité et particulièrement mis en avant par la jurisprudence lorsqu'il est question de contrôles de données de communications[860].

De nouvelles interprétations pourraient venir, d'une part, d'un arrêt de la grande chambre de la Cour européenne des droits de l'homme dans une affaire *Bărbulescu c. Roumanie* qui dégage des balises plus précises quant aux principes à respecter en matière de communications électroniques et, d'autre part, du règlement général sur la protection des données qui entre en application après la période analysée. Le RGPD jette un coup de projecteur sur la protection des données et pourrait davantage être mobilisé par les plaideurs et les juridictions. Toujours est-il que durant la période analysée, on a pu recenser des appréciations assez diverses des exigences à respecter en matière de contrôle, notamment en regard d'une distinction entre communications professionnelles et privées que certaines juridictions mettent davantage en exergue.

Cette insécurité juridique se prolonge dans les débats relatifs à la recevabilité de la preuve lorsque la juridiction conclut à une violation des dispositions applicables. Comme nous le verrons dans la section 5 sur ce point là aussi les appréciations sont variables.

a. Le contrôle et la prise de connaissance de messages électroniques et de données de navigation

163. Le contrôle d'une messagerie instantanée devant la Cour européenne des droits de l'homme[861]. En 2016, un arrêt de la Cour strasbourgeoise dans une affaire opposant M. Bărbulescu à la Roumanie a créé le débat en ce qu'il pouvait être interprété comme limitant la protection

855 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 », *R.D.T.I.*, 2015, n° 59, pp. 103-108 ; « 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, n° 48, pp. 127-145 ; « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, 2009, n° 35, pp. 126-140.

856 Essentiellement en référence à l'article 8 de la CEDH et à la jurisprudence de la Cour européenne des droits de l'homme.

857 Loi du 8 décembre 1992.

858 Art. 124 et 125 de la loi sur les communications électroniques et art. 314*bis* du Code pénal.

859 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.

860 Voy. not. C. trav. Liège (div. Neufchâteau, 8e ch.), 13 septembre 2017, R.G. n° 2016/AU/32, disponible sur www.terralaboris.be.

861 Cette partie reprend des extraits de K. Rosier, « La Cour européenne se débat avec la question du contrôle des messages électroniques sur le lieu du travail », *B.S.J.*, 2016/558, p. 5 et K. Rosier, « Contrôle des communications électroniques du travailleur : l'affaire *Bărbulescu* revue et corrigée par la Grande Chambre de la Cour Européenne des Droits de l'Homme », *B.S.J.*, 2017, n° 594, p. 4.

du travailleur concernant la surveillance des communications électroniques dont il pouvait faire l'objet dans le contexte professionnel[862].

À l'origine du litige, un contrôle d'un compte de messagerie instantanée sur lequel il y avait eu quelques échanges privés avec des membres de la famille de M. Bărbulescu et dont certains avaient trait à la vie sexuelle de ce dernier. Un second compte de messagerie électronique Yahoo Messenger, créé antérieurement et tout à fait privé, avait également été contrôlé. L'employeur avait, pendant plusieurs jours, enregistré systématiquement les communications électroniques et avait opéré une transcription de celles-ci. Il avait, suite à une interpellation de Monsieur Bărbulescu, invité celui-ci à préciser s'il utilisait ou non à des fins privées le compte de messagerie, ce à quoi Monsieur Bărbulescu avait répondu par la négative, ignorant que son employeur disposait d'une transcription de ses communications. L'utilisation des ressources informatiques à des fins privées en contravention des règles d'entreprise (et non la teneur des messages) avait ensuite conduit au licenciement du travailleur.

Dans son arrêt du 12 janvier 2016, la Cour avait constaté l'existence d'une ingérence dans la vie privée du travailleur mais avait conclu que celle-ci était admissible, notamment en raison du fait que ce contrôle avait eu lieu alors que les messages étaient censés être de nature professionnelle et que les juridictions roumaines avaient estimé que le contrôle s'inscrivait dans le cadre d'un contrôle disciplinaire permis par le Code du travail roumain. Certains auteurs y voyaient un recul par rapport à la jurisprudence antérieure de la Cour surtout en raison du peu d'égard accordé au critère de proportionnalité de la mesure de contrôle[863]. En effet, si on peut comprendre qu'un employeur conserve des moyens de contrôle, l'arrêt pouvait laisser penser que, du fait que l'employeur avait interdit tout usage privé des outils de communications, il pouvait ainsi exercer une surveillance des plus intrusives, et ce alors qu'il n'y avait aucun indice de manquement grave qui le justifiait et qu'il n'était pas même établi que le travailleur avait été averti de la nature et de la portée de ces mesures de contrôle[864].

C'est dire l'intérêt avec lequel on attendait l'arrêt de la grande chambre. Son arrêt du 7 septembre 2017[865] adopte une position assez différente de celle qui vient d'être rappelée et elle ne fait d'ailleurs pas l'unanimité puisque 7 juges ont émis une opinion dissidente sur les conclusions de cet arrêt[866]. Il n'en demeure pas moins qu'il est certain que l'arrêt rendu est un arrêt de principe important, et ce à plusieurs égards.

862 Cour eur. D.H., 12 janvier 2016, *Bărbulescu c. Roumanie*, req. n° 61496/08. Pour des commentaires de cet arrêt, voy. not. J.-P. Maguénaud et J. Mouly, « Big Boss is watching you – Alerte sur le contrôle des activités électroniques du salarié. Obs. sous Cour eur. D.H., arrêt *Bărbulescu c. Roumanie*, 12 janvier 2016 », *Rev. trim. dr. h.*, 2016/108, p. 1037 ; K. Rosier, « La Cour européenne se débat avec la question du contrôle des messages électroniques sur le lieu du travail », *B.S.J.*, 2016/558, p. 5.

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

864 Lire à cet égard l'opinion partiellement dissidente du juge Pinto De Albuquerque à la suite de l'arrêt du 12 janvier 2016, *Bărbulescu c. Roumanie*, req. n° 61496/08, § 3.

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

866 Opinion dissidente des juges Raimondi, Dedov, KjØlbro, Mits, Mourou-Vikström et Eicke à la suite de l'arrêt *Bărbulescu c. Roumanie*,

Tout d'abord, concernant l'appréciation de l'existence d'une ingérence dans la vie privée et dans la correspondance au travail, la Cour rappelle que le fait que la correspondance soit échangée dans un contexte professionnel n'empêche pas l'application de l'article 8 de la CEDH[867]. Il convient toutefois de vérifier s'il y a eu ingérence en l'espèce, en particulier au regard des attentes raisonnables de ce dernier. Et c'est sur ce point que la Cour adopte une position forte. Nonobstant la conclusion selon laquelle il n'y avait peut-être pas d'attentes raisonnables en matière de vie privée dans le chef de M. Bărbulescu dans la mesure où il avait été informé du fait qu'il lui était interdit d'utiliser l'outil informatique de l'employeur à des fins privées et qu'une travailleuse avait fait l'objet d'un licenciement pour non-respect de ces règles d'entreprise, la Cour va considérer que l'employeur ne peut réduire à néant le droit à une vie sociale au travail en donnant des instructions qui autoriseraient un contrôle sans limite par les instructions qu'il donne.

La Cour va donc conclure qu'en l'espèce, il y a bien ingérence dans la vie privée et la correspondance du travailleur.

Ensuite, la Cour développe une méthodologie inédite par rapport à sa jurisprudence antérieure sur ces questions pour apprécier le caractère admissible ou non de l'ingérence. La particularité de l'affaire Bărbulescu est qu'elle opposait un employeur du secteur privé à un travailleur. Il s'agissait donc de faire l'application horizontale de la CEDH. La Cour relève que la législation en matière de droit du travail de la plupart des États membres du Conseil de l'Europe laisse une grande autonomie aux parties au contrat de travail pour définir leurs droits et obligations mutuels. Elle constate d'ailleurs qu'il y a peu d'États européens qui ont légiféré de façon spécifique en ce qui concerne la surveillance des communications électroniques sur les lieux du travail.

Elle ne va dès lors pas orienter sa réflexion sur l'existence d'un cadre normatif qui permettait en l'occurrence de protéger le travailleur, mais plutôt vérifier si les juridictions du travail, saisies du litige au niveau national, ont correctement interprété les exigences découlant de l'article 8 de la CEDH dans leur analyse du litige. Ce faisant, elle court-circuite en quelque sorte les dispositions nationales pour vérifier si différents critères ont été respectés lors du contrôle des communications. Ces critères ont trait à l'information fournie préalablement concernant les mesures de surveillance, au caractère justifié et proportionné de ces mesures par rapport à un objectif qui doit être légitime dans le chef de l'employeur[868], à la proportionnalité des mesures prises suite au contrôle ainsi qu'à l'existence de mesures adéquates devant notamment permettre d'empêcher que l'employeur ait accès au contenu des communications en cause sans que le travailleur n'ait été préalablement averti d'une telle éventualité[869].

En l'espèce, la grande chambre va estimer que l'examen réalisé par les juridictions nationales a été trop léger et qu'il n'a pas été vérifié quelles étaient concrètement les raisons légitimes qui avaient poussé l'employeur à contrôler toutes les communications de M. Bărbulescu pendant plusieurs

867 Cour eur. D.H. (gr. ch.), 7 septembre 2017, *Bărbulescu c. Roumanie*, req. n° 61496/08, § 71.

868 À cet égard, la Cour reconnaît qu'un employeur a un intérêt légitime à assurer le bon fonctionnement de l'entreprise, ce qui peut se traduire par la mise en place des mécanismes lui permettant de vérifier que ses employés accomplissent leurs tâches professionnelles « de manière adéquate et avec la célérité requise » (Cour eur. D.H. (gr. ch.), 7 septembre 2017, *Bărbulescu c. Roumanie*, req. n° 61496/08, § 127).

869 *Ibid.*, § 121.

jours. Ce dernier n'avait en effet évoqué aucun risque particulier qui aurait nécessité qu'une telle surveillance soit mise en place[870].

Cet arrêt nous semble donc important en ce qu'il consacre un « espace vital » pour l'échange de communications électroniques sur le lieu du travail. Il n'impose pas à l'employeur de fournir des outils de communication mais il consacre le droit, lorsque ces outils existent, à un minimum de protection indépendamment des règles d'entreprise qui sont définies à cet égard. Ensuite, il donne des critères beaucoup plus précis sur des règles minimales à respecter par l'employeur en termes de contrôle en fournissant une grille d'analyse que le juge national devrait prendre en compte lorsqu'il vérifie la compatibilité d'un contrôle qui a été mis en œuvre par rapport à l'article 8 de la CEDH.

Cela laisse présager sans doute d'un avant et d'un après dans le cadre des jurisprudences nationales qui devront, à notre sens, prendre en compte ces principes, indépendamment des règles peut-être moins protectrices en vigueur dans le droit national.

164. La jurisprudence de la Cour européenne des droits de l'homme appliquée par une juridiction belge. La jurisprudence en Belgique a donné un écho à ce deuxième arrêt dans un arrêt du 13 septembre 2017 de la cour du travail Liège, division Neuchâteau[871].

La cour se réfère à l'arrêt du 7 septembre 2017 de la Cour européenne des droits de l'homme pour en retenir que l'article 8 de la CEDH implique, lorsqu'il est question de contrôle de communications électroniques du travailleur, le respect des principes suivants :

- « les salariés doivent être informés de manière claire quant à la nature de la surveillance et préalablement à sa mise en place ;
- une distinction doit être faite entre flux et contenu des communications. Si la surveillance du contenu est opérée par une méthode invasive, elle doit être sérieusement justifiée. Il convient aussi de se demander si des moyens moins intrusifs auraient pu être utilisés et qu'elles ont été les conséquences de la surveillance pour l'employé concerné ;
- les autorités doivent vérifier que l'employé s'est vu offrir des garanties adéquates qui permettent d'empêcher qu'un employeur n'ait accès au contenu même des communications, sans que l'employé n'ait été préalablement averti d'une telle éventualité ».

Quant à l'intégration de ces exigences dans le droit interne, la cour rappelle que si cette réglementation interne satisfait à ces exigences, il convient d'appliquer ces règles internes sauf si l'article 8 de la CEDH garantit un degré supérieur de protection, et la cour de rappeler que l'article 8 peut être invoqué directement et, entre particuliers, devant les juridictions belges.

La cour va ensuite considérer que les règles édictées par la CCT n° 81 intègrent les principes de l'article 8 de la CEDH. Elle considère que « pour que l'ingérence de l'employeur relève de l'exercice normal de l'autorité patronale, la cour doit vérifier la régularité des contrôles sur la base des principes de légalité (ou transparence), de finalité et de proportionnalité, en tenant compte de la portée du consentement donné par la travailleuse lorsqu'elle fut informée par écrit [en l'occurrence par un règlement de travail] et préalablement des possibles contrôles ».

870 *Ibid.*, § 133.

871 C. trav. Liège (div. Neufchâteau, 8e ch.), 13 septembre 2017, R.G. n° 2016/AU/32, disponible sur www.terralaboris.be.

Dans le cas tranché, il était question d'un licenciement suite à la prise de connaissance par l'employeur d'un e-mail échangé entre la travailleuse et son époux et dont le contenu était insultant à l'égard de l'employeur. La cour va relever que l'employeur n'établit pas que le contrôle a été mis en œuvre dans le cadre d'une des finalités prévues dans la CCT n° 81 et reprises dans le règlement de travail et qu'en outre, l'employeur n'avait pu cibler cet e-mail qu'au terme d'un examen systématique de mails privés dans la boîte mail professionnelle de la travailleuse, ce qui conférait au contrôle un caractère disproportionné. Pour ces motifs, la cour va considérer que la preuve a été obtenue de manière irrégulière[872].

Avant le second arrêt *Bărbulescu*, la jurisprudence s'est prononcée à plusieurs reprises et dans des sens diverses sur la question de la régularité de la prise de connaissance de données de communications électroniques, qu'il s'agisse de données de communications téléphoniques, de courriers électroniques ou encore de données de navigation sur internet.

165. Contrôle des courriers électroniques et des données de navigation au regard du seul article 8 CEDH. Dans un arrêt du 22 juin 2016, la cour du travail de Mons a eu à connaître de l'accès à des e-mails du collaborateur ainsi qu'à la consultation de son historique de navigation[873]. Après rupture de la collaboration, l'ancien manager engagé dans le cadre d'un contrat d'entreprise sollicitait la requalification de la convention en contrat de travail et réclamait également une indemnisation pour la prise de connaissance d'e-mails privés et d'autres informations liées à la consultation de sites internet et de Facebook sur des équipements appartenant à l'entreprise. L'entreprise avait en effet commenté dans deux e-mails, adressés postérieurement à la fin du contrat ses trouvailles, sur le PC et dans la boîte mail anciennement utilisés par le collaborateur.

La cour va considérer qu'il n'y a pas lieu à requalification. Elle analyse dès lors la question de la consultation des données, non à l'aune de la CCT n° 81, mais sous l'angle de l'article 8 de la CEDH en rappelant l'exigence d'un respect du droit au respect de la vie privée même à l'égard de communications effectuées via du matériel de l'entreprise. Elle conclut au caractère fautif de la prise de connaissance des données en raison du non-respect de l'exigence de légalité (il n'y avait aucun règlement interne régissant l'usage et le contrôles des outils de communication concernés) et des principes de finalité et de proportionnalité (l'entreprise ne pouvait justifier cette prise de connaissance au regard d'un but légitime). Elle condamne la société au paiement d'un montant de 1.000 euros à titre de dommages et intérêts.

166. Contrôle de la boîte mail professionnelle – Transparence et exigence de consentement. Dans un arrêt du 4 août 2016, la 4e chambre de la cour du travail de Bruxelles se prononce sur certains aspects de la problématique des e-mails sur le lieu du travail[874]. Le travailleur faisait valoir que le contrôle de son PC portable avait été effectué de façon irrégulière soulignant le fait qu'il avait été sommé de se soumettre à un contrôle en présence d'un huissier et de remettre ce PC portable, sans qu'on puisse en déduire un consentement véritable dans son chef. Il invoquait une violation de l'article 314*bis* du Code pénal, de l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques qui consacre le principe du secret des communications élec-

872 Pour ce qui est de la recevabilité de cette preuve, voy. *infra*, section 5.

873 C. trav. Mons (8e ch.), 22 juin 2016, *J.T.T.*, 2017, p. 114.

874 C. trav. Bruxelles (4e ch.), 4 août 2016, *J.T.T.*, 2016, p. 391. Pour un commentaire de cette décision, voy. K. Rosier, « Du neuf en matière de jurisprudence *Antigone* en matière contractuelle ? », *B.S.J.*, 2017, n° 579, p. 6.

troniques et de la CCT n° 81 qui réglemente le contrôle des e-mails et de l'internet sur le lieu du travail.

La cour rappelle que l'article 314*bis* du Code pénal ne s'applique que pendant la transmission de la communication et n'avait en toute hypothèse pas lieu d'être invoqué dans le cadre du litige qui lui avait été soumis. Par rapport à l'article 124 de la loi du 13 juin 2005, la cour énonce que cette disposition est applicable aux communications professionnelles et que l'article 17, 2°, de la loi relative aux contrats de travail ne constitue pas une base légale suffisante pour autoriser le contrôle des communications électroniques par l'employeur dans le cadre des exceptions prévues à l'article 125 de cette loi[875].

Elle considère, par ailleurs, que le fait que l'employeur ait indiqué dans l'*IT policy* de l'entreprise que l'ordinateur portable n'était mis à disposition qu'à des fins professionnelles n'implique pas que la CCT n° 81 a été respectée, l'employeur n'établissant pas avoir respecté ses obligations de transparence concernant la politique de contrôle des données de communications électroniques.

La cour va considérer que dès lors que la société en question n'avait pas respecté la CCT n° 81, ni l'article 124 de la loi du 13 juin 2005, l'employeur a porté atteinte à un droit fondamental du travailleur. Elle en conclut que la preuve est irrégulière.

C'est une solution opposée qui se dégage d'un arrêt d'une autre chambre de la cour du travail de Bruxelles du 17 janvier 2017[876]. La cour considère que la prise de connaissance de courriers électroniques qui ont un caractère professionnel – non privé selon les termes de la Cour – ne peut enfreindre ni l'article 22 de la Constitution, ni la loi du 8 décembre 1992, ni l'article 124 de la loi sur les communications électroniques, de sorte qu'il est sans intérêt de vérifier si le travailleur concerné a ou non donné son accord pour que l'employeur accède à ces courriers[877].

167. Contrôle du contenu de courriers électroniques professionnels – Champ d'application de la CCT n° 81. Dans un arrêt du 9 septembre 2016, une autre chambre de la cour du travail de Bruxelles met en exergue une particularité du champ d'application de la CCT n° 81[878]. Elle considère que la prise de connaissance par l'employeur du contenu des courriers électroniques d'un travailleur dans sa boîte mail professionnelle ne relève pas du champ d'application de la CCT n° 81 dès lors que la convention ne vise que le contrôle *des données de communication* (ce qui correspond à l'adresse de l'expéditeur, du destinataire, la date et heure d'envoi essentiellement). Selon la cour, la prise de connaissance du *contenu* du message relève de l'article 8 de la CEDH et

875 Ce point est controversé, certains auteurs estimant que la loi n'est pas suffisamment précise (voy. not. J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », in *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, pp. 85-86 et O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, p. 51) et une partie de la jurisprudence (voy. not. C. trav. Mons, 25 novembre 2009, *R.D.T.I.*, 2010, p. 81, note K. Rosier) à laquelle s'est ralliée la Commission de la protection de la vie privée dans son rapport juridique sur la cybersurveillance de 2012 (p. 13) estimant au contraire que le contrôle des communications électroniques peut relever de l'exercice normal du contrôle patronal normal tel qu'il découle de la loi sur le contrat de travail.

876 C. trav. Bruxelles, 17 janvier 2017, R.G. n° 2014/AB/1028, *Ors.*, 2017 (reflet B. Paternostre), liv. 8, 24 ; *Or.*, 2017 (reflet B. Paternostre), liv. 10, 27.

877 Dans le même sens, voy. C. trav. Liège (div. Namur, 6e ch.), R.G. n° 2016/AN/117, inédit ; C. trav. Mons (3e ch.), 22 décembre 2015, R.G. n° 2013/AM/335, www.juridat.be.

878 C. trav. Bruxelles (3e ch.), 9 septembre 2016, R.G. n° 2015/AB/624, www.juridat.be.

de l'article 124 de la loi du 13 juin 2005 sur les communications électroniques. En réalité, les partenaires sociaux avaient estimé que le contrôle du contenu des communications électroniques était excessif, raison pour laquelle seul le contrôle des données des communications est organisé par la CCT. Ils avaient dès lors subordonné le contrôle du contenu au consentement des parties à la communication, et certainement à celui du travailleur, conformément au prescrit des lois du 21 mars 1991 (remplacée par la loi du 13 juin 2005) et du 8 décembre 1992[879].

168. Redirection des courriers électroniques sans l'accord du destinataire. Dans un arrêt du 6 janvier 2016, la cour du travail de Bruxelles considère que le droit au respect de la vie privée d'une travailleuse n'est pas violé du fait que son adresse professionnelle a été automatiquement déviée vers celle d'un autre membre du personnel sans accord exprès de la travailleuse concernée[880]. Il se fonde exclusivement sur la considération selon laquelle, dès lors qu'il s'agissait d'une boîte professionnelle, la travailleuse ne pouvait se plaindre du fait que des messages privés aient été concernés par ce transfert dans la mesure où cela supposait qu'elle ait elle-même pris le risque de communiquer cette adresse à ses contacts privés. Le raisonnement suivi est lapidaire et ne s'appuie pas sur les dispositions légales en la matière.

169. Usage d'un e-mail envoyé à partir d'une adresse privée. Dans un litige de licenciement d'un fonctionnaire, ce dernier contestait l'utilisation, dans le dossier constitué pour prendre cette décision, d'e-mails adressés par ce dernier à partir de son adresse privée. Il invoquait une violation de la loi du 8 décembre 1992, notamment du fait que les copies papier d'e-mails avaient été prises dans son bureau alors qu'il était absent. Le Conseil d'État va relever que ces documents se trouvaient dans des dossiers emportés par ses supérieurs hiérarchiques et qu'ils devaient être considérés comme faisant partie du dossier fiscal[881]. Il relève également que l'objet des courriers était bien lié au travail du fonctionnaire, même s'il avait utilisé une autre adresse pour les envoyer. Il en conclut que la loi du 8 décembre 1992 ne fait en l'occurrence pas obstacle à ce que ces courriers soient pris en compte dans le cadre de la procédure qui a conduit au licenciement. Il est à noter que l'argumentation de la décision ne permet pas de déterminer ce qui l'amène à considérer que l'application de la loi du 8 décembre 1992 n'invalide pas l'usage de ces e-mails. Le fait que des e-mails revêtent un caractère professionnel n'empêche en effet pas l'application de cette législation.

170. Communication à des fins de preuve d'un courrier électronique dont on est le destinataire. Dans un arrêt du 22 avril 2015, la Cour de cassation a constaté qu'aucune disposition légale ne s'oppose à la production d'un courrier électronique régulièrement reçu par son destinataire et communiqué à la justice à des fins de preuves[882]. Cette conclusion s'appuie sur le fait que les dispositions qui interdisent la prise de connaissance ou l'enregistrement de communications électroniques ne s'applique pas à la personne qui est partie à la communication[883].

879 Préambule de la CCT n° 81, p. 5.

880 C. trav. Bruxelles (4e ch.), 6 janvier 2016, *J.L.M.B.*, 2016, p. 171.

881 C.E. (9e ch.), 29 décembre 2015, *Stefan Longueville c. Belgische Staat*, n° 233.366.

882 Cass. (2e ch.), 22 avril 2015, *J.T.*, 2015, p. 634.

883 Voy. concl. av. gén. D. Vandermeersch, précédant Cass. (2e ch.), 22 avril 2015, *J.T.*, 2015, p. 633. En ce sens également à propos d'un enregistrement d'une conversation téléphonique : Corr. Brabant wallon (ch. cons.), 24 avril 2017, inédit.

b. Contrôle des données d'appels téléphoniques

171. Contrôle des données d'appels téléphoniques – Application de la CCT n° 81. Dans un arrêt du 10 juin 2015, la cour du travail de Mons s'est penchée sur le respect de la législation applicable en matière d'obtention de preuves consistant en des données de communications téléphoniques et de navigation sur internet[884]. Il était fait grief au travailleur licencié d'avoir appelé de manière répétée et excessive (près de 5 h 30 de communications sur un mois) un numéro surtaxé qui correspondait à un service de rencontre pour homosexuels. La particularité était que ces appels avaient été passés à partir d'un poste fixe qui n'était pas celui du travailleur. Il s'agissait de celui d'un bureau occupé principalement par une autre personne, mais les appels étaient passés lorsque cette personne était absente. Constatant un surcoût à la réception de la facture, l'employeur avait cherché à identifier l'auteur des appels. En confrontant les données indiquant la présence du travailleur licencié, l'employeur avait été vérifier dans les relevés d'appels du GSM utilisé par le travailleur s'il avait déjà appelé ce numéro surtaxé. Fort du constat que deux appels avaient été passés par le travailleur vers ce numéro et après avoir également par ailleurs recueilli des données concernant la consultation de sites internet par ce travailleur que l'employeur associait à ce numéro de téléphone, l'employeur avait estimé disposer d'une connaissance suffisante des faits pour licencier le travailleur pour motif grave.

La cour considèrera que les actes posés violent le droit au respect de la vie privée du travailleur et la loi du 8 décembre 1992. Elle préconise qu'au vu de la complexité du cadre légal en vigueur, le caractère licite ou non du contrôle soit apprécié à l'aune des critères de légalité, transparence, finalité et proportionnalité. Dans le cours de cette analyse, elle constate que si la finalité du contrôle est légitime, et ce d'autant plus que le règlement de travail interdisait l'usage abusif du téléphone professionnel, un défaut d'information préalable concernant le contrôle des données de communications passées via le GSM et le contrôle des données de navigation sur internet. Elle estime également que le contrôle était disproportionné parce que, d'une part, la vérification des données de communication a porté sur une période antérieure au contrôle trop longue et, d'autre part, il y a eu individualisation immédiate des données. Ce dernier point est sans doute inspiré d'une exigence de la CCT n° 81 en matière de contrôle des données de communications qui prévoit que lorsque l'employeur effectue un contrôle pour s'assurer du respect des règles d'utilisation qu'elle a définies, il ne peut immédiatement individualiser les données. Il doit d'abord procéder à une phase d'avertissement préalable, ce qui n'avait pas été le cas en l'espèce. Relevons toutefois que l'application de la CCT n° 81 au contrôle des données de communications téléphoniques est discutable et que d'autres décisions antérieures n'en font pas application et considèrent que l'employeur, en tant qu'abonné, peut légitimement contrôler les données de communications figurant sur les factures qu'il reçoit[885].

La cour conclut donc au caractère illicite de la collecte de la preuve[886].

884 C. trav. Mons (8e ch.), 10 juin 2015, *J.T.T.*, 2016, p. 77. Pour un commentaire : K. Rosier, « Le délicat exercice de la collecte d'informations personnelles préalable à un licenciement », *B.S.J.*, 2017, n° 559, pp. 1-2.

885 C. trav. Gand (div. Gand, 2e ch.), 12 mai 2014, *J.T.T.*, 2014, p. 320 ; *R.W.*, 2014-2015, liv. 40, p. 1586 ; Trib. trav. Bruxelles (3e ch.), 16 septembre 2004, *J.T.T.*, 2005, p. 61 ; C. trav. Liège, 21 mai 2001, *J.T.T.*, 2002, p. 180 ; C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2002, p. 41.

886 Sur la recevabilité de ces preuves, voy. *infra*, section 5.

c. Les enregistrements audio de communications téléphoniques

172. Enregistrements à l'insu de l'interlocuteur. Dans un arrêt du 17 novembre 2015[887], la Cour de cassation a réaffirmé sa jurisprudence antérieure[888] aux termes de laquelle elle 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 lorsque la personne enregistrée pouvait légitimement nourrir des attentes raisonnables en matière de respect de sa vie privée. La Cour indique que ni l'article 8.1 de la CEDH ni l'article 314*bis* du Code pénal n'interdisent le simple enregistrement d'une conversation par un participant à cette conversation à l'insu des autres participants. Elle précise que « celui qui, en vue de l'administration de la preuve dans un litige impliquant les participants à une conversation, fait usage d'un enregistrement effectué par lui de cette conversation à laquelle il a pris part, n'agit pas avec l'intention frauduleuse ou le dessein de nuire visés par l'article 314*bis*, § 2, alinéa 2, du Code pénal. Toute utilisation de l'enregistrement, hors le cas de la simple utilisation pour soi-même et à la différence de l'utilisation visée à l'article 314*bis*, § 2, alinéa 2, du Code pénal, peut toutefois constituer une atteinte à l'article 8 de la Convention »[889].

Pour ce qui est de l'appréciation du critère des atteintes raisonnables, la Cour précise qu'il doit être appliqué tant en ce qui concerne les participants à la conversation, que pour ce qui touche à l'objectif de l'utilisation de l'enregistrement. Elle ajoute qu'« [à] cet égard, la teneur de la conversation, les circonstances dans lesquelles cette conversation a eu lieu, la qualité des participants et la qualité du destinataire de l'enregistrement peuvent notamment jouer un rôle ». À noter que dans le cas soumis à la Cour de cassation, il était également question de secret professionnel dès lors que l'enregistrement litigieux visaient les propos d'un avocat et avait été réalisé par son client. La Cour va encore préciser que « [l]e secret professionnel pénalement sanctionné par l'article 458 du Code pénal n'interdit pas à un client d'enregistrer une conversation ayant lieu dans le cabinet de son conseil entre lui-même, son conseil et un tiers et d'utiliser cet enregistrement si cela s'avère nécessaire à sa défense dans une procédure pénale engagée notamment contre ce conseil ».

C'est également dans la lignée de cette jurisprudence que, dans un arrêt du 25 novembre 2015, la cour du travail de Bruxelles écarte des débats des enregistrements de conversations électroniques réalisés pendant la relation de travail par le travailleur à l'insu de ses interlocuteurs au motif de la violation de leur droit à la vie privée[890]. La cour s'appuie sur les enseignements dégagés de l'arrêt de la Cour de cassation en matière d'attentes raisonnables pour considérer que les personnes enregistrées n'avaient pas été averties que leurs propos pourraient être écoutés par des tiers ou produits en tant que preuves en justice[891].

887 Cass. (2e ch.), 17 novembre 2015, R.G. n° P.15.0880.N.

888 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.

889 Voy. également l'arrêt du 7 juin 2016 qui réaffirme ce principe (Cass. (2e ch.), 7 juin 2016, R.G. n° P.16.0294.N).

890 C. trav. Bruxelles (4e ch.), 25 novembre 2015, R.G. n° 2011/AB/612, disponible sur www.terralaboris.be.

891 L'arrêt fait toutefois référence à l'arrêt de la Cour de cassation du 9 septembre 2008 et non à l'arrêt du 17 novembre 2015 auquel il est pratiquement concomitant. Dans le même sens et se fondant sur l'arrêt du 17 novembre 2017, voy. Trib. trav. Liège (div. Liège, 4e ch.), 20 mars 2017, disponible sur www.terralaboris.be. Dans ce jugement, le tribunal conclut à la violation du droit au respect de la vie privée mais admet la preuve en application de la jurisprudence *Antigone*.

173. Incidence de la qualité de la personne qui enregistre la communication. La chambre du conseil du tribunal de première instance du Brabant wallon a constaté que, dès lors que c'est une personne partie à l'entretien téléphonique qui enregistre la communication, cet enregistrement ne constitue par une infraction aux articles 314*bis*, § 2, alinéa 1er, du Code pénal ni à l'article 124, § 4, de la loi du 13 juin 2005 relative aux communications électroniques[892].

174. Incidence du contexte de l'enregistrement. Dans la même affaire, il était reproché à la travailleuse auteur de l'enregistrement d'avoir traité des données à caractère personnel en effectuant cet enregistrement sans respecter les dispositions de la loi du 8 décembre 1992, et singulièrement l'obligation d'information. La chambre du conseil va estimer que dès lors que l'enregistrement intervient après le licenciement de la travailleuse, dans le but de pouvoir établir le véritable motif de celui-ci, il s'agit d'un traitement relevant de l'exclusion du champ d'application de la loi prévue à l'article 3, § 2, de celle-ci pour les traitements effectués à des fins exclusivement personnelles ou domestiques, de sorte qu'un tel enregistrement n'est pas soumis à l'application de cette loi[893].

d. Prise de connaissance de propos sur les réseaux sociaux

175. Prise de connaissance de propos publiés sur les réseaux sociaux. La jurisprudence recensée concernant des motifs de licenciement liés à des propos tenus sur Facebook[894] ou à des opinions exprimées par des « like »[895] ne se penche pas sur la recevabilité des preuves. La question de la régularité de la prise de connaissance de données de communication ne fait pas débat, même lorsque les propos sont rapportés à l'employeur par des collègues du travailleur qui en est l'auteur[896] (laissant donc penser que les propos ne sont pas accessibles au public). La question de l'accessibilité des propos soit à un nombre plus ou moins important de personnes[897], soit à certaines personnes concernées par ceux-ci[898], est toutefois soulignée pour évaluer la gravité de la faute reprochée au travailleur[899].

892 Corr. Brabant wallon (ch. cons.), 24 avril 2017, inédit.

893 *Ibid.*

894 C. trav. Bruxelles (4e ch.), 24 juin 2015, R.G. n° 2013/AB/922, *Chron. D.S.*, 2016/9, pp. 390-393 ; C. trav. Liège (3e ch.), 16 février 2016, R.G. n° 2015AL-264, *Sem. soc. / Soc. week.*, 2017/3 ; C.E., 25 octobre 2016, n° 236.264, cité par F. Lambinet, « Propos inappropriés et provocateurs sur Facebook : un manquement au devoir de réserve du fonctionnaire », *B.S.J.*, n° 588, 2017, p. 6.

895 C. trav. Liège (div. Liège, 3e ch.), 24 mars 2017, R.G. n° 2016/AL/94, inédit.

896 C. trav. Liège (3e ch.), 16 février 2016, R.G. n° 2015AL-264, *Sem. soc. / Soc. week.*, 2017/3.

897 Dans un arrêt du 24 juin 2015, la cour du travail de Bruxelles prend en compte le fait que la travailleuse licenciée pouvait légitimement penser que ses propos n'étaient visibles que par un destinataire (C. trav. Bruxelles (4e ch.), 24 juin 2015, R.G. n° 2013/AB/922, *Chron. D.S.*, 2016/9, pp. 390-393).

898 Les collègues de travail de la personne licenciée (C. trav. Liège (3e ch.), 16 février 2016, R.G. n° 2015AL-264, *Sem. soc. / Soc. week.*, 2017/3).

899 La cour du travail de Liège, division Liège, a considéré que le fait pour un membre du personnel de « liker » sur son profil Facebook des liens vers un site véhiculant des publications polémiques à connotation raciste alors que son employeur est une ASBL à vocation d'intégration sociale et que l'employé en question avait déjà fait l'objet de mises en garde, est fautif (C. trav. Liège (div. Liège, 3e ch.), 24 mars 2017, R.G. n° 2016/AL/94, inédit).

2. Les fichiers stockés sur un support appartenant à l'entreprise

176. Contrôle de fichiers sur le disque dur. Dans un jugement du 25 avril 2016, le tribunal du travail du Hainaut, division Mons, se penche sur la question de la violation de la CCT n° 81 à propos de la prise de connaissance de documents à caractère privé du travailleur stockés sur le réseau informatique de l'entreprise[900]. Il met tout d'abord en évidence qu'il n'est pas établi que l'employeur ait accédé au PC du travailleur. Les documents étant sauvegardés sur le serveur de l'entreprise, ce dernier pouvait techniquement y avoir accès à partir d'un autre poste.

Le tribunal indique encore que le seul fait que l'employeur découvre sur ce serveur des documents Word privés d'un travailleur ne suffit pas à démontrer l'existence d'une violation du droit au respect de la vie privée de ce dernier. Lorsqu'il est question de fichiers Word ou autres qui ne relèvent pas du domaine des communications électroniques (courriers électroniques, connexions internet), la jurisprudence n'applique pas la CCT n° 81 qui régit 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[901].

C'est au regard du droit au respect de la vie privée de l'article 8 de la CEDH et 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 qu'il convient de raisonner. La combinaison de ces deux textes implique, en bref, le respect d'un principe de transparence (qui se traduit dans la loi du 8 décembre 1992 par une obligation d'information préalable), de légitimité et de proportionnalité du contrôle.

C'est faisant application de ces mêmes critères que la cour du travail de Liège, division Namur, va se prononcer sur le cas d'une prise de connaissance du contenu d'un disque dur en présence du travailleur et d'un huissier de justice[902]. Soupçonnant un travailleur d'avoir lancé une activité concurrente et d'avoir enregistré des fichiers concernant cette activité sur le disque dur de l'ordinateur mis à sa disposition par l'entreprise, un employeur avait demandé à ce travailleur d'accéder, en présence d'un huissier, à des fichiers non identifiés comme étant privés sur cet ordinateur. La cour va estimer qu'au vu des circonstances (le travailleur n'a pas été contraint, n'a émis aucune réserve et les fichiers consultés ne relevaient pas de la sphère privée), il n'y a pas eu d'ingérence au droit au respect de la vie privée dudit travailleur[903].

3. Géolocalisation

177. Exigence d'une proportionnalité. Dans une décision du 13 février 2015, le tribunal du travail d'Anvers, division Malines, se prononce sur l'utilisation par l'employeur d'un système de monitoring de véhicules professionnels couplé à un système de géolocalisation[904]. Le tribunal

900 Trib. trav. Hainaut (div. Mons), 25 avril 2016, R.G. n° 14/3775/A, inédit, cité par K. Rosier, « Correspondance privée sauvegardée sur le serveur de l'entreprise : à quoi s'attendre ? », *B.S.J.*, 2016/567, p. 6.

901 Ainsi, dans un arrêt du 26 novembre 2014, la cour du travail de Liège, division de Neufchâteau, a écarté l'application de la CCT n° 81 pour le contrôle de fichiers se trouvant sur le disque dur d'un PC (C. trav. Liège (div. Neufchateau, 11e ch.), 26 novembre 2014, R.G. n° 2011/AU/24, inédit). Voy. en ce sens également : C. trav. Bruxelles (3e ch.), 14 octobre 2011, R.G. n° 2010/AB/1029, www.juridat.be.

902 C. trav. Liège (div. Namur, 13e ch.), 17 novembre 2015, *Chron. D.S.*, 2016, p. 204.

903 Voy. également sur l'application de ces critères par la Cour européenne des droits de l'homme, l'arrêt *Libert c. France* qui sera commenté dans la prochaine chronique (Cour eur. D.H., 22 février 2018, *Libert c. France*, req. n° 588/13).

904 Trib. trav. Anvers (sect. Malines, 3e ch.), 13 février 2015, n° 13/1775/A, *Chron. D.S.*, 2015, liv. 1, 18, note N. Tine.

examine la légalité du recours à un tel système à l'aune des principes de finalité légitime, de proportionnalité et de transparence, qui découlent de l'article 8 de la CEDH et de l'application de la loi du 8 décembre 1992 aux traitements effectués par de tels dispositifs. En l'occurrence, dans la lignée de la jurisprudence précédente[905], le tribunal va considérer que le système ne satisfait pas aux exigences de proportionnalité car il était actif même en dehors des heures de travail.

178. Exigence d'une information préalable. Toujours dans la même affaire[906], le tribunal retient comme fondé le fait que l'employeur ne démontrait pas avoir suffisamment informé les travailleurs des particularités du système installé et des finalités d'utilisation par l'employeur. Dans le même sens, la cour du travail de Liège, division Liège, a rejeté comme preuve des données de géolocalisation utilisées par l'employeur pour démontrer que le travailleur licencié n'avait pas presté chez un client les heures qu'il avait déclarées, et ce au motif que l'employeur n'apportait pas la preuve d'une information préalable donnée au travailleur sur l'installation du système, conforme aux exigences de l'article 9 de la loi du 8 décembre 1992[907].

179. Dispositif installé par un détective privé dans un véhicule privé. Une autre affaire retiendra notre attention. La cour du travail de Gand a eu à trancher un cas dans lequel un détective privé avait installé, dans le cadre d'une mission confiée par l'employeur, un système de géolocalisation dans le véhicule personnel d'un travailleur soupçonné de mener une activité concurrentielle à celle de l'employeur[908]. Le travailleur dont question avait sollicité le retrait en portant plainte à la police avant son licenciement. La cour constate qu'il n'y a aucune base légale autorisant un employeur, fût-ce par l'intermédiaire d'un détective privé, à placer un dispositif de géolocalisation dans un véhicule n'appartenant pas à l'employeur sans le consentement du travailleur. Au contraire, un tel acte constitue une atteinte flagrante au droit au respect de la vie privée du travailleur.

4. Vidéosurveillance

180. Vidéosurveillance d'un lieu public. Dans un arrêt du 18 mars 2016, la cour du travail de Liège a considéré que la captation et l'utilisation d'images de vidéosurveillance par des caméras installées dans un lieu public (magasin de grande surface et parking de celui-ci) ne violaient pas le droit au respect de la vie privée du travailleur qui avait été filmé en train de voler du matériel dès lors que ledit travailleur avait été parfaitement informé du placement de ces caméras[909]. Sur l'incidence du caractère public des lieux, signalons qu'un arrêt de la Cour européenne des droits de l'homme du 28 novembre 2017 a considéré que le fait que les caméras se trouvent installées dans un lieu accessible au public (amphithéâtre d'une université) n'impliquait pas en soi qu'il n'y avait pas d'ingérence dans la vie privée lorsque c'était un lieu d'échanges entre professeurs et étudiants[910]. Elle a considéré que les enseignants pouvaient nourrir des attentes raisonnables

905 C. trav. Gand, 14 octobre 2011, *J.T.T.*, 2012, p. 190 ; *Ors.*, 2012 (reflet I. Plets), liv. 2, 32 ; *Or.*, 2012 (reflet I. Plets), liv. 2, p. 6.

906 Trib. trav. Anvers (sect. Malines, 3e ch.), 13 février 2015, n° 13/1775/A, *Chron. D.S.*, 2015, liv. 1, 18, note N. Tine.

907 C. trav. Liège (div. Liège, 3e ch.), 8 novembre 2017, R.G. n° 2016/AL/772, www.juridat.be. À noter que cette décision examine également la légalité d'un système de badges enregistrant les dates et heures d'entrées et de sorties des bâtiments à des fins de vérification du temps de travail sous l'angle de l'application de la loi du 8 décembre 1992.

908 C. trav. Gand (div. Gand, 2e ch.), 2 mars 2016, *T.G.R.-T.W.V.R.*, 2016, liv. 4, 312.

909 C. trav. Liège (3e ch.), 18 mars 2016, *J.T.T.*, 2016, pp. 283-285.

910 Cour eur. D.H., 28 novembre 2017, *Antović et Mirković c. Monténégro*, req. n° 70838/13.

quant au fait que leurs propos ne soient tenus que pour les personnes physiquement présentes et ne fassent pas l'objet d'un enregistrement systématique, même si celui-ci avait été porté à leur connaissance[911]. Cette décision a toutefois fait l'objet d'une opinion dissidente des juges Pano, Bianku et Kjolbro qui ont insisté à la fois sur le caractère accessible au public des lieux et sur le caractère limité de la vidéosurveillance (en ce que l'accessibilité et la conservation des images étaient tout à fait limitées) pour considérer qu'il n'y avait pas d'ingérence dans la vie privée des enseignants.

181. Vidéosurveillance du processus de production. Dans un jugement du 13 mars 2017[912], le tribunal du travail de Liège rappelle les conditions d'information préalable et de limitation quant à la surveillance par caméra d'une chaîne de production en application de la loi du 8 décembre 1992 et de la Convention collective de travail n° 68[913]. Un employeur entendait prouver qu'un travailleur licencié avait saboté une partie de la ligne de la production par des images issues des caméras de vidéosurveillance. Le tribunal va estimer que la preuve produite est irrégulière dès lors que l'employeur n'établit pas avoir respecté les conditions de traitement de la CCT n° 68 dont le non-respect est sanctionné pénalement. Il n'était pas établi que les informations prescrites à l'article 9 de la CCT et destinées aux organes de représentation des travailleurs leur avaient été fournies. Elle constate également que les caméras filmaient en continu alors que l'article 6, § 3, de la CCT prévoit que la surveillance ne peut être que temporaire lorsque la finalité de celle-ci vise le contrôle du processus de production des travailleurs[914].

182. Utilisation d'une caméra cachée par l'employeur. De manière assez prévisible, la cour du travail de Bruxelles a, dans un arrêt du 2 octobre 2015, considéré que des images filmées par le biais d'une caméra cachée n'ont pas été obtenue de manière régulière dès lors que la Convention collective de travail n° 68 impose une information préalable[915]. Dans son appréciation quant à la recevabilité de la preuve que nous commenterons plus avant *infra* sous la section 5, elle considère même que le fait que l'employeur ait prétendu auprès des travailleuses concernées qu'il s'agissait d'un hygromètre digital est contraire à l'article 16, § 1er, de la loi relative aux contrats de travail qui impose une obligation de respect et d'égards mutuels entre parties. C'est une appréciation différente des conséquences du non-respect de la CCT n° 68 que fait le tribunal de première instance de Flandre orientale, division Gand, dans une décision du 25 mai 2016[916]. Le tribunal considère que l'absence d'information préalable peut certes constituer une violation de la CCT n° 68 mais que la preuve recueillie est recevable dès lors notamment que la violation n'entache pas la fiabilité de la preuve.

911 La Cour évoque toutefois la possibilité de dérogations ponctuelles lors d'enregistrements prévus pour les besoins de l'enseignement (par exemple, si des étudiants ne peuvent être physiquement présents). L'admissibilité de l'ingérence n'a pas fait l'objet d'une analyse approfondie de la Cour dès lors qu'elle a d'emblée constaté que les juges du fond, ayant conclu à l'absence d'ingérence, n'avaient pas vérifié l'existence d'une base légale. Cette condition d'admissibilité n'ayant pas été rencontrée, cela a suffi à la Cour pour constater la violation de l'article 8 de la CEDH.

912 Trib. trav. Liège (div. Liège, 4e ch.), 13 mars 2017, R.G. n° 16/6.097/A, disponible sur www.terralaboris.be.

913 Convention collective de travail n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail.

914 Le jugement se prononce également sur la recevabilité de la preuve irrégulière (pour un commentaire, *cfr infra*, section 5).

915 C. trav. Bruxelles (3e ch.), 2 octobre 2015, R.G. n° 2014/AB/103, www.juridat.be.

916 Civ. Flandre orientale (div. Gand), 25 mai 2016, www.juridat.be.

183. Captation d'images vidéo de l'employeur par le travailleur. La cour du travail de Bruxelles a rendu un arrêt du 7 janvier 2015[917] à propos de l'usage d'une caméra cachée par un travailleur. Ce dernier 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 sur le contrat de travail.

5. Recevabilité des preuves

184. Tendances générales concernant la recevabilité des preuves irrégulièrement recueillies. On constate une division plus marquée dans la jurisprudence en matière de recevabilité de la preuve et, plus particulièrement, lorsqu'il s'agit d'appliquer ou non la jurisprudence *Antigone*.

Pour rappel, cette jurisprudence de la Cour de cassation tire son nom d'un arrêt du 14 octobre 2003[918] rendu en matière pénale. La Cour de cassation y opère un renversement de la règle de l'exclusion des preuves recueillies illicitement. Progressivement et aux travers de différents arrêts, la Cour a dégagé un principe selon lequel le juge doit avoir égard aux 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 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. Il est notamment question d'une proportionnalité entre la gravité de la violation qui conduit à constater l'irrégularité de la preuve (qui, dans la matière analysée, réside généralement dans une violation du droit au respect de la vie privée) avec la gravité du manquement que la preuve entend établir.

Nous avions constaté dans les précédentes chroniques une adoption de cette jurisprudence en droit social après une réticence des juges du fond, surtout suite à un arrêt du 10 mars 2008 de la Cour rendu à propos d'une sanction de chômage imposée par l'Onem sur la base d'informations illicitement communiquées à cet organisme[919].

Pour ce qui concerne l'évolution de la jurisprudence durant la période examinée, nous avons relevé des décisions qui considèrent que la jurisprudence trouve à s'appliquer en matière de contrat de travail et d'autres décisions qui rejettent l'application de celle-ci sur la base de différentes argumentations.

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

918 Cass. (2e ch.), 14 octobre 2003, R.G. n° P.03.0762.N, www.cass.be, concl. av. gén. De Swaef.

919 Cass., 10 mars 2008, *Or.*, 2008, p. 172, note I. Plets ; *J.L.M.B.*, 2009, p. 580, note R. De Baerdemaeker.

Parmi les décisions qui font application de la jurisprudence *Antigone*, peu concluent, au terme de l'application des trois critères rappelés *supra*, que la preuve doit être acceptée[920].

a. Jurisprudence faisant application de la jurisprudence Antigone

185. Transposition des critères *Antigone* en matière civile. La cour du travail de Mons se prononce à plusieurs reprises pour l'application de la jurisprudence *Antigone* en matière civile[921]. Dans un arrêt du 18 avril 2016, la cour estime que les critères de cette jurisprudence sont transposables à la matière civile pour autant que la notion de manquement soit substituée à celle d'infraction[922].

186. Critère de la fiabilité. La cour du travail de Mons a, dans un arrêt du 10 juin 2015, fait application de la jurisprudence *Antigone* à des preuves dont elle avait jugé qu'elles avaient été recueillies de manière illicite (données de communications téléphoniques)[923]. Elle écarte les éléments produits concernant les numéros appelés par le travailleur grâce à son GSM. Elle estime que l'illicéité commise entache la fiabilité de la preuve au motif que les recherches effectuées pour confondre le travailleur ont été orientées et n'ont pas visé d'autres travailleurs qui auraient pu potentiellement être impliqués.

C'est également notamment le caractère non fiable de la preuve qui a amené la cour du travail de Bruxelles à considérer que des images caméra obtenues en violation de la CCT n° 68 devaient être écartées des débats au motif que l'employeur avait manipulé les enregistrements en ne produisant que des extraits choisis sur trois jours d'enregistrement[924].

Dans le même sens, la cour du travail de Mons a considéré que des propos recueillis par un détective privé, sans information préalable, impliquaient une irrégularité entachant la crédibilité de la preuve[925]. Cet arrêt s'inscrit dans le contexte de l'application de la loi du 8 décembre 1992 aux détectives privés et en particulier de l'article 9 de cette loi. La cour a tenu compte des circonstances particulières de la cause. Il s'agissait de déterminer si le décès d'un travailleur avait eu lieu sur le chemin du travail ce qui avait amené l'assureur à remettre en cause le fait que le travailleur résidait à l'adresse de sa compagne au départ de laquelle il avait débuté son trajet. La cour a mis en exergue le contexte émotionnel postérieur au décès et le fait que la déclaration de la compagne obtenue par le détective avait pu être orientée puisque celle-ci n'était pas informée de la finalité pour laquelle elle était recueillie. La cour conclut que la violation (absence d'information préalable) entache la crédibilité de la preuve et porte atteinte au droit à un procès équitable en ce qu'elle induit une violation du droit de la défense.

920 Voy. toutefois Trib. trav. Liège (div. Liège, 4e ch.), 20 mars 2017, disponible sur www.terralaboris.be.

921 C. trav. Mons (8e ch.), 10 juin 2015, *J.T.T.*, 2016, p. 77 ; C. trav. Mons (2e ch.), 18 avril 2016, R.G. n° 2015/AM/101, inédit, commenté par S. Gilson, « Les détectives privés et Antigone : des liaisons dangereuses », *B.S.J.*, 2016/566, p. 6.

922 C. trav. Mons (2e ch.), 18 avril 2016, R.G. n° 2015/AM/101, inédit, commenté par S. Gilson, « Les détectives privés et Antigone : des liaisons dangereuses », *B.S.J.*, 2016/566, p. 6.

923 C. trav. Mons (8e ch.), 10 juin 2015, *J.T.T.*, 2016, p. 77. Voy. commentaire de cette décision, *supra*, le n° 171.

924 C. trav. Bruxelles (3e ch.), 2 octobre 2015, R.G. n° 2014/AB/103, www.juridat.be.

925 C. trav. Mons (2e ch.), 18 avril 2016, R.G. n° 2015/AM/101, inédit, commenté par S. Gilson, « Les détectives privés et Antigone : des liaisons dangereuses », *B.S.J.*, 2016/566, p. 6.

187. Caractère disproportionné de l'atteinte à la vie privée. Dans un arrêt du 9 septembre 2016, la 3e chambre de la cour du travail de Bruxelles considère que la jurisprudence *Antigone* est applicable à l'appréciation de la recevabilité de courriers électroniques obtenus en violation de l'article 8 de la CEDH et de l'article 124 de la loi sur les communications électroniques[926]. Faisant application de l'un des critères évoqués par la Cour de cassation dans son arrêt du 2 mars 2005[927], elle considère que la prise de connaissance de communications privées se trouvant dans une boîte mail professionnelle sans le consentement des personnes concernées est une illicéité commise et est sans commune mesure avec le manquement qu'il est censé permettre de constater.

À noter que cette cour avait déjà considéré dans un autre arrêt que l'usage d'une caméra cachée présentée à des travailleuses comme un hygromètre digital impliquait une violation des droits de ces dernières, violation qui était disproportionnée par rapport aux manquements que les images produites tendaient à prouver, dès lors qu'il ne s'agissait pas d'établir une infraction[928]/[929].

C'est également le fait que les preuves avaient été obtenues d'une manière qui implique une atteinte disproportionnée au droit au respect de la vie privée d'une travailleuse qui conduit la cour du travail de Liège, division Neufchâteau, dans un arrêt du 13 septembre 2017 à écarter des preuves jugées préalablement comment ayant été obtenues de manière irrégulière[930]. Point intéressant de la décision, celle-ci s'emploie à resituer la jurisprudence *Antigone* dans un contexte plus global. Elle relève que les problèmes d'insécurité juridique posés par la jurisprudence *Antigone* limitée aux trois critères qui ont été dégagés par celle-ci pour déterminer si une preuve irrégulière doit ou non être déclarée recevable doivent être résolus sur la base des indications contenues dans toute la jurisprudence, et principalement de la Cour européenne des droits de l'homme pour ce qui concerne l'article 8 de la CEDH, et de la Cour de cassation. La cour se propose dès lors d'analyser la problématique en vérifiant si le droit d'une partie de présenter devant le juge des preuves recueillies de manière illégale (ou déloyale) doit l'emporter sur le droit de son adversaire au respect de ses droits fondamentaux, en examinant tous les éléments spécifiques à la cause.

La cour considérera que la preuve – e-mail échangé par la travailleuse avec son époux – a été obtenue par le biais d'une intrusion délibérée et irrégulière dans la boîte mail de la travailleuse et que cela induit une atteinte grave dans la sphère privée de la travailleuse, d'autant qu'en l'espèce le courrier en question était échangé dans le contexte d'une relation de confiance entre deux conjoints, sans qu'une publicité ne soit donnée, en dehors du couple, aux propos échangés. La cour relève que « ceci aboutit à créer les conditions d'une fouille illégale permettant de glaner des motifs de rupture qui n'ont d'autres contenus que ce qui relève de la sphère privée assumée dans le seul cadre conjugal. En quelque sorte, la fouille soutenue irrégulièrement de courriels privés constitue la matrice du grief, viciant le processus dès sa genèse ». La balance des intérêts en présence conduit la cour à déclarer la preuve irrecevable.

926 C. trav. Bruxelles (3e ch.), 9 septembre 2016, R.G. n° 2015/AB/624, www.juridat.be.

927 Il s'agit de l'arrêt dit « Manon » : Cass. (2e ch.), 2 mars 2005, R.G. n° P.04.1644.F.

928 C. trav. Bruxelles (3e ch.), 2 octobre 2015, R.G. n° 2014/AB/103, www.juridat.be.

929 Dans un sens contraire mais impliquant la preuve d'une infraction pénale : Civ. Flandre orientale (div. Gand), 25 mai 2016, www.juridat.be.

930 C. trav. Liège (div. Neufchâteau, 8e ch.), 13 septembre 2017, R.G. n° 2016/AU/32, disponible sur www.terralaboris.be. Voy. *supra*, n° 164 pour un commentaire de la décision concernant cette irrégularité.

b. Jurisprudence rejetant l'application de la jurisprudence Antigone

188. Limitation de la jurisprudence *Antigone* à la matière pénale. Dans un arrêt du 6 février 2015, la cour du travail de Liège a considéré dans un litige relatif à l'indemnisation d'un accident de travail qu'« [i]l n'y a pas lieu de résoudre cette question de légalité par une application extensive de la jurisprudence *Antigone* en dehors de la sphère dans laquelle la jurisprudence de la Cour de cassation l'a cantonnée jusqu'à présent : celle du contentieux pénal et celle de litiges du droit de la sécurité sociale dans lesquels sont constatées des infractions pénales commises par des assurés sociaux ou des infractions aux obligations réglementaires de déclaration précise et complète de leur situation de revenus ou d'activités, réprimées par des sanctions d'exclusion de prestations sociales qui revêtent un caractère de nature pénale au sens de la jurisprudence de Strasbourg en la matière »[931].

Dans le prolongement de cet arrêt sur lequel il s'appuie, le tribunal du travail de Liège a considéré dans un jugement du 13 mars 2017[932] qu'il n'y avait pas lieu de résoudre la question de la recevabilité d'une preuve en dehors de la sphère pénale au regard de la jurisprudence *Antigone*. Le tribunal opère également une mise en perspective de la jurisprudence et de la pertinence des critères qu'elles prônent pour sanctionner ou non l'irrégularité de la preuve. Elle relève qu'en l'espèce, s'agissant d'une violation de la CCT n° 68 passible de sanctions pénales, la sanction est plus importante que la sanction de nullité reprise comme critère de l'application de la jurisprudence *Antigone* et rappelle que le droit au respect de la vie privée est un droit fondamental qui s'applique également sur le lieu du travail.

189. Arguments tirés d'autres arrêts. Toujours dans la même décision du 13 mars 2017[933], le tribunal pointe l'arrêt de la Cour de cassation du 13 décembre 2016 rendu en matière pénale[934] qui casse un arrêt de la cour d'appel d'Anvers en matière d'infraction de roulage au motif d'une violation de la législation en matière de protection des données. Le tribunal y voit une forme de sanction directe de l'irrégularité d'une preuve en matière pénale obtenue en violation de la législation sur la protection des données. Dans un arrêt du 4 août 2016, la cour du travail de Bruxelles estime dans le même sens que la jurisprudence de la Cour de cassation doit être interprétée comme ayant une portée limitée dans la mesure où si elle peut se « justifier par le souci d'assurer l'efficacité de la répression administrative au pénal des infractions commises dans ces matières, son extension sans limite aux relations contractuelles de pur droit privé risquerait d'aboutir à une transgression systématique des dispositions sanctionnées pénalement qui protègent la vie privée, dans le seul but d'établir des fautes ou des comportements, qui, quant à eux, ne sauraient laisser prise à la qualification d'infraction pénale »[935].

931 C. trav. Liège (div. Liège, 6e ch.), 6 février 2015, R.G. n° 2013/AL/392, www.juridat.be. Pour un commentaire de cette décision : K. Rosier, « Détectives privés et vie privée : mener l'enquête, mais pas en toute discrétion », in *Recueil de jurisprudence : responsabilité – assurances – accidents du travail*, Limal, Anthemis, 2015, pp. 35-55.

932 Trib. trav. Liège (div. Liège, 4e ch.), 13 mars 2017, R.G. n° 16/6.097/A, disponible sur www.terralaboris.be.

933 Trib. trav. Liège (div. Liège, 4e ch.), 13 mars 2017, R.G. n° 16/6.097/A, disponible sur www.terralaboris.be.

934 Cass. (2e ch.), 13 décembre 2016, R.G. n° P.16.0682.N. Pour un commentaire de cet arrêt, voy. la section D. Commission de la protection de la vie privée à propos de l'e-gouvernement (Coline Fievet, Loïck Gérard et Julie Mont), *infra*.

935 C. trav. Bruxelles (4e ch.), 4 août 2016, *J.T.T.*, 2016, p. 391. Voy. commentaire de cette décision sous le n° 166 *supra*.

La Cour se prévaut également, dans son argumentation, d'un arrêt de la Cour de justice du 17 février 2015[936]. Cet arrêt avait été rendu en matière fiscale à propos de la régularité de preuves obtenues dans le cadre d'une enquête pénale (interceptions de télécommunications et de saisies de courriers électroniques) et transmises à l'administration fiscale. Dans cet arrêt, la Cour de justice va considérer que si la juridiction nationale saisie constate que des preuves qui lui sont soumises ont été obtenues dans le cadre de la procédure pénale ou utilisées dans celui de la procédure administrative en violation de l'article 7 de la Charte des droits fondamentaux de l'Union européenne relatif au droit au respect de la vie privée et familiale, ladite juridiction nationale doit écarter ces preuves[937].

La cour du travail s'appuie sur un commentaire de cet arrêt de Monsieur F. Koning[938] pour considérer que ladite décision non seulement « sonne le glas de la transposition en matière fiscale de la jurisprudence "*Antigone*", mais a une portée qui va au-delà de la seule sphère fiscale et déborde également sur la jurisprudence pénale "*Antigone*" proprement dite, en réaffirmant le principe de la stricte légalité de la preuve comme critère d'écartement de la preuve recueillie irrégulièrement »[939].

190. Argument tiré de l'égale valeur des droits et liberté en présence. Dans le même sens, la cour du travail de Liège, division Liège, rejette l'application de la jurisprudence *Antigone* en matière de contrat de travail lorsqu'il est question de non-respect du droit au respect de la vie privée[940]. Dans un arrêt du 8 novembre 2017, elle relève que la jurisprudence *Antigone* « met à néant le principe de légalité du contrôle, de l'ingérence et neutralise les règles de procédure et les balises prévues par les dispositions légales et les conventions collectives ». Elle considère également que, « en droit du travail, le conflit de valeurs se présente en outre dans une même sphère d'intérêts privés et de droits et devoirs réciproques sans qu'aucun critère objectif ou fondamental ne justifie de privilégier le respect de l'un ou l'autre sous peine d'arbitraire. Le respect des principes constitutionnels et légaux et de leurs balises quant à l'ingérence possible (légalité, finalité, proportionnalité et transparence) est le seul garant de la sécurité juridique ».

D. La Commission de la protection de la vie privée et l'e-gouvernement (Coline Fievet, Loïck Gérard et Julie Mont)

1. L'e-gouvernement

191. Tentatives de définition. Si la doctrine définit l'e-gouvernement comme « l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi

936 C.J.U.E., 17 décembre 2015, *WebMindLicenses Kft.*, aff. C-419/14, *J.T.*, 2016, p. 401, note F. Koning ; *T.F.R.*, 2016, p. 342, note P. De Vos et D. Verbeke.

937 *Ibid.*, § 91.

938 F. Koning, « Mort de la transposition en matière fiscale de la jurisprudence pénale *antigone* ? », *J.T.*, 2016, p. 397.

939 Notons toutefois qu'une décision ultérieure du Tribunal de l'Union européenne du 8 septembre 2016 (arrêt *Goldfish*) rendue en matière de concurrence s'aligne sur la jurisprudence de la Cour européenne des droits de l'homme, sans faire cas de l'arrêt de la Cour de justice évoqué ci-avant, ce qui rend d'autant plus difficile de conclure à l'existence d'une jurisprudence claire à ce sujet au niveau du droit de l'Union. Pour un commentaire des deux décisions, voy. D. Mougenot, « Antigone au milieu du gué. Le point sur l'utilisation de preuves recueillies irrégulièrement en matière civile », in C. Delforge (dir.), *La preuve en droit privé : Quelques questions spéciales*, Bruxelles, Larcier, 2017, pp. 127-177.

940 C. trav. Liège (div. Liège, 3e ch.), 8 novembre 2017, R.G. n° 2016/AL/772, www.juridat.be.

que les mutations que ces utilisations engendrent »[941], on remarque que la notion – bien qu'explicitement mentionnée dans diverses législations – n'est guère définie par le législateur[942].

Qu'en est-il pour la Commission de la protection de la vie privée[943] ? Si, à l'instar du législateur, la C.P.V.P. ne délimite pas clairement et précisément les contours de la notion d'e-gouvernement, force est de constater que la Commission y rattache certains principes. Ainsi, à l'occasion de deux avis portant sur des avant-projets de décrets relatifs à la gestion du paiement des allocations familiales[944], la C.P.V.P. rappelle l'existence des trois principes d'e-gouvernement suivants : la collecte unique de données (i), l'utilisation de sources authentiques (ii), ainsi que la mise à disposition et l'accès à ces sources authentiques via des intégrateurs de services (iii). En outre, la C.P.V.P. recommande aux demandeurs d'avis qui recourent à ces principes de les mentionner explicitement et en utilisant exclusivement les termes susmentionnés (collecte unique, source authentique, intégrateurs de service) et non des expressions ou termes *sui generis* propres à chaque législation[945]. Si la Commission ne définit pas l'e-gouvernement en tant que tel, elle élabore et défend l'existence d'un vocabulaire commun désignant les principes applicables à cette matière.

Les lignes qui suivent synthétisent les principaux avis que la C.P.V.P. a rendus entre 2015 et 2017 au sujet des outils et principes d'e-gouvernement ainsi que les applications concrètes de ceux-ci en matière d'administration numérique.

2. Les outils et principes d'e-gouvernement

a. Les sources authentiques comme outils d'e-gouvernement

192. Notion. Les sources authentiques de données occupent, avec les intégrateurs de services, une place importante dans le développement de l'e-gouvernement et plus particulièrement du principe de collecte unique des données des citoyens. Concrètement, la source authentique de données prend la forme d'une base de données dont l'alimentation et la gestion sont assurées par une autorité publique déterminée. Cette base de données est ensuite rendue accessible – sous conditions – à d'autres acteurs publics, évitant ainsi des sollicitations multiples auprès des citoyens. La création et l'utilisation de sources authentiques par les pouvoirs publics ayant un impact important sur la vie privée des citoyens, la C.P.V.P. est appelée à se prononcer sur la conformité de celles-ci avec la législation vie privée.

193. Procédure de désignation d'une source authentique. Saisie d'une demande d'avis par l'intégrateur de services fédéral Fedict, la C.P.V.P. a eu l'occasion d'examiner la nécessité de

941 E. Degrave, *L'e-gouvernement et la protection de la vie privée : légalité, transparence et contrôle*, Bruxelles, Larcier, 2014, p. 33.

942 Voy. par exemple l'article 2 de l'accord de coopération du 26 août 2013 entre les administrations fédérales, régionales et communautaires afin d'harmoniser et d'aligner les initiatives visant à réaliser un e-gouvernement intégré, *M.B.*, 8 octobre 2013.

943 Ci-après, « C.P.V.P. » ou « Commission ».

944 C.P.V.P., avis n° 412017 du 26 juillet 2017 relatif à un avant-projet de décret (de la Région flamande) réglant l'octroi des allocations dans le cadre de la politique de la famille ; C.P.V.P., avis n° 51/2017 du 20 septembre 2017 relatif à un avant-projet de décret relatif au nouveau dispositif mis en place en Région wallonne pour la gestion et le paiement des prestations familiales.

945 C.P.V.P., avis n° 41/2017 du 26 juillet 2017, précité, n^{os} 11 et 12 ; C.P.V.P., avis n° 51/2017 du 20 septembre 2017, précité, n^{os} 6 et 7.

déterminer des critères permettant de qualifier une donnée d'authentique[946]. Malgré le caractère favorable de son avis, la Commission émet certaines remarques et s'interroge, de manière plus fondamentale, sur le fait qu'une « réglementation excessive » de la procédure de désignation de sources authentiques « aille à l'encontre » de la mise en place effective de tels outils[947]. Parmi les remarques de fond formulées par la C.P.V.P., la plus importante concerne l'absence totale de transparence en ce qui concerne la désignation d'une autorité en tant que responsable/gestionnaire de source authentique. Ce manque de transparence empêche les pouvoirs publics d'avoir « une vue claire des sources et données authentiques qu'ils peuvent/doivent consulter pour l'exercice de leurs missions » et ne permet pas aux personnes concernées « de savoir quels organismes assurent la gestion de leurs données reprises dans les sources authentiques afin de savoir auprès de qui exercer leur droit d'accès et éventuellement leur droit de rectification »[948]. Afin de pallier ce manque de transparence, la Commission suggère à l'intégrateur de services fédéral de « dresser, tenir à jour et assurer la publicité de la liste des différentes sources authentiques […] reconnues au niveau fédéral ainsi que des données authentiques y reprises »[949].

194. Banque de données issues de sources authentiques. En 2016, la C.P.V.P. se prononce sur la création par le législateur wallon d'une banque de données issues de sources authentiques[950]. Cet avis est l'occasion pour la Commission de rappeler, via un renvoi à l'accord de coopération du 23 mai 2013[951], les spécificités de cet instrument. Ainsi, une banque de données issues de sources authentiques est « une base de données instituée par une disposition décrétale, regroupant un ensemble de données issues de sources authentiques ou de liens entre des données issues de sources authentiques et dont la collecte, le stockage, la mise à jour et la destruction sont assurés exclusivement par une autorité publique déterminée, appelée gestionnaire de banque de données issues de sources authentiques, et qui sont destinées à être réutilisées par les autorités publiques »[952]. Au vu de cette définition, la principale différence pratique entre une banque de données issues de sources authentiques et une « simple » source authentique réside dans le fait que l'autorité publique responsable de la gestion de cette banque de données est amenée à effectuer des mises en commun, des agrégations et des consolidations de données provenant de sources authentiques diverses afin de fournir une information plus complète et transversale aux destinataires de données. Compte tenu de ces missions supplémentaires, la Commission souligne

946 C.P.V.P., avis n° 20/2015 du 10 juin 2015 relatif au projet d'arrêté royal déterminant les critères sur la base desquels les 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.

947 *Ibid.*, n° 8.

948 *Ibid.*, n° 18.

949 *Ibid.*, n° 34.

950 C.P.V.P., avis n° 39/2016 du 20 juillet 2016 relatif à un avant-projet de décret portant octroi d'aides, au moyen d'un portefeuille intégré d'aides de la Wallonie, aux porteurs de projets et aux petites et moyennes entreprises pour rémunérer des services promouvant l'entrepreneuriat ou la croissance, et constituant une banque de données de sources authentiques liées à ce portefeuille intégré.

951 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, *M.B.*, 23 juillet 2013.

952 C.P.V.P., avis n° 39/2016, précité, n° 5.

l'importance qu'un service spécifique et disposant de moyens suffisants soit désigné en tant que gestionnaire d'une telle banque de données[953].

195. Sources authentiques et protection de la vie privée. Par son avis 49/2017 du 20 septembre 2017, la Commission se prononce sur un avant-projet de loi créant la Banque de données centrale des actes de l'état civil (BAEC)[954]. La BAEC est une source authentique[955] « qui intègre les registres communaux existants et les postes consulaires dans une seule banque de données centralisée »[956]. Cet avis est l'occasion pour la Commission de mettre en œuvre son examen du respect, par la source authentique, de la législation vie privée. Ainsi, la C.P.V.P. constate que la source authentique poursuit des finalités déterminées, explicites et légitimes qui sont directement inscrites dans le texte de l'avant-projet de loi[957]. La Commission constate ensuite que les données reprises dans la BAEC sont décrites de manière suffisamment précise[958] et que ces données sont « adéquates, pertinentes et non excessives » eu égard aux finalités poursuivies[959]. La C.P.V.P. constate ensuite que les exigences en termes de durée de conservation des données, de désignation d'un gestionnaire de la source authentique et d'adoption de mesures techniques et organisationnelles à même de garantir un traitement sur des données sont globalement atteintes[960]. Étrangement, la Commission ne semble guère s'intéresser à l'existence d'éventuelles mesures visant à garantir l'exercice des droits des personnes concernées. Au terme de son analyse, la C.P.V.P. émet un avis favorable à la création de la BAEC.

b. La protection des données du citoyen

i. Registre national des personnes physiques

196. Données communiquées volontairement. En 2015, la C.P.V.P. est amenée à rendre un avis sur un avant-projet de loi modifiant la loi du 8 août 1993 organisant le Registre national[961]. Malgré un avis favorable, la Commission formule certaines remarques, comme le fait que, si le Registre national peut contenir des données transmises par les citoyens, la loi doit impérativement faire ressortir le caractère volontaire de la transmission d'informations par ces citoyens. Près de deux ans plus tard, le ministre de l'Intérieur a demandé un avis de la C.P.V.P. sur le projet d'arrêté royal qui avait précisément pour objet de déterminer quelles données peuvent être communiquées volontairement par les citoyens et le mode de transmission de celles-ci. Si la Commission reste favorable au principe de conservation et d'enregistrement de données communiquées volontairement par les citoyens, ce sur la base du consentement de ceux-ci, un avis défavorable

953 *Ibid.*, nos 16 et 17.

954 C.P.V.P., avis no 49/2017 du 20 septembre 2017 relatif à un avant-projet de loi portant dispositions diverses en matière de droit civil.

955 Le concept de banque de données issues de source authentique n'étant pas présent dans la législation fédérale, la banque de données centrale des actes de l'état civil est – malgré une dénomination qui peut sembler trompeuse – une source authentique.

956 C.P.V.P., avis no 49/2017, précité, no 3.

957 *Ibid.*, no 6.

958 *Ibid.*, nos 10 à 12.

959 *Ibid.*, no 14.

960 *Ibid.*, nos 15 et s.

961 C.P.V.P., avis no 15/2015 du 13 mai 2015 au sujet de l'avant-projet de loi portant des dispositions diverses concernant des secteurs relevant des attributions « Intérieur ».

a par contre été rendu sur le contenu de ces données et la manière dont les citoyens peuvent les communiquer/modifier et sur le procédé de suppression des données par les administrations communales et les services du Registre national[962].

197. Fichier de journalisation. Suite à des plaintes et questions émanant des citoyens au sujet des consultations du Registre national par les autorités communales, la C.P.V.P. a émis deux recommandations à destination de celles-ci en 2015 (par l'intermédiaire de son Comité sectoriel du Registre national) et en 2017. Pour pouvoir garantir un encadrement de l'accès au Registre national des citoyens, la C.P.V.P. a recommandé, à l'aune des principes de responsabilité et de transparence des traitements, un contrôle adéquat des finalités pour lesquelles le Registre national est consulté par les villes et communes (i), un enregistrement des motifs de la consultation (ii), une journalisation de chaque consultation ou mise à jour du Registre (iii) et la fourniture d'informations complètes, via un fichier de journalisation complet, en cas d'exercice de son droit d'accès par un citoyen (iv)[963].

ii. Domicile numérique

198. Introduction dans le Code civil envisagée. L'article 102 du Code civil consacre le domicile comme étant le lieu où tout Belge a son principal établissement. Le domicile numérique, inspiré par l'utilisation de plus en plus prégnante des moyens de communication électroniques par les citoyens, consiste en un lieu de rencontre et d'échange dématérialisé avec l'État. Fin mars 2017, la Commission est saisie d'une demande d'avis du président de la Chambre concernant une proposition de loi relative à l'introduction, dans le Code civil, du domicile numérique[964]. L'exposé des motifs évoque la volonté de « centraliser les communications de toutes les autorités publiques dans une boîte de réception unique, de sorte que le destinataire peut prendre connaissance, via un seul point de contact, des documents et messages de différentes autorités »[965]. Cette proposition s'inscrit pleinement dans la mouvance de l'e-gouvernement et la stratégie digitale d'ici 2020, en ce qu'elle vise notamment à simplifier les interactions entre citoyens et autorités publiques. La communication par voie électronique – via une adresse e-mail – avec l'Administration implique *de facto* un traitement de données à caractère personnel, devant s'analyser au regard du régime de protection prévu par le nouveau règlement européen[966].

962 C.P.V.P., avis n° 04/2017 du 11 janvier 2017 au sujet du projet d'arrêté royal déterminant les données de contact visées à l'article 3, alinéa 1er, 17°, de la loi du 8 août 1993.

963 C.P.V.P., Comité sectoriel du Registre national, recommandation RN n° 01/2015 du 18 février 2015 aux communes et administrations locales relative à la sécurité de l'information devant encadrer leurs accès au Registre national et traitements consécutifs des données du Registre national ; C.P.V.P., recommandation n° 07/2017 du 30 août 2017 aux villes et communes concernant l'enregistrement du motif de la consultation du Registre national par les membres de leur personnel.

964 C.P.V.P., avis n° 28/2017 du 24 mai 2017 concernant la proposition de loi relative à l'introduction, dans le Code civil, du domicile numérique.

965 Proposition de loi relative à l'introduction, dans le Code civil, du domicile numérique, exposé des motifs, *Doc. parl.*, sess. 2016-2017, n° 2112/001, p. 7.

966 Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.* L 119/1 du 4 mai 2016.

Après avoir rappelé qu'elle soutient l'implémentation de nouvelles techniques de communication dans le but d'améliorer l'efficacité ainsi que le service aux administrés[967], la Commission émet cependant des réserves concernant la mise en œuvre concrète de l'outil proposé. Elle met tout d'abord en garde contre l'utilisation, à son sens inadéquate, de la notion de domicile. En effet, la proposition de loi semble faire fi des « conséquences (juridiques spécifiques) » y attachées[968]. La question de l'absence de considérations quant à la sécurisation de la boîte électronique est ensuite évoquée[969]. Ainsi, elle insiste sur la responsabilité de l'expéditeur du courriel en termes de sécurité des données jusqu'au moment de leur réception par le destinataire. C'est finalement l'exigence de consentement qui appelle les plus amples commentaires. Selon la Commission, il convient de privilégier la définition consacrée à l'article 1er, § 8, de la loi vie privée[970]. La proposition de loi mentionnant un consentement explicite, « la Commission interprète […] dans le sens qu'un acte positif spécifique de la personne concernée est requis »[971]. Étant donné que la modification proposée implique une manifestation de volonté de la part du citoyen d'activer ou pas sa boîte électronique, des situations problématiques sont à prévoir. La Commission prend l'exemple de la possibilité, pour un usager, de contester la réception d'un document contenant une décision lui étant préjudiciable[972]. Elle argue en sus que, s'il existe déjà une e-Box sécurisée pour les citoyens qui permet la délivrance de certains documents, son succès est limité. Les usagers mobilisent en effet plus souvent leur boîte e-mail dans le cadre d'échanges d'ordre privé tels que les factures d'eau ou de téléphonie[973]. Finalement, elle estime que le rendement du système proposé serait « médiocre » et rend un avis défavorable[974].

3. *Les applications concrètes en matière d'administration numérique*

a. L'informatisation de la justice

199. Contexte. Entre 2015 et 2017, le législateur fédéral a édicté, à travers diverses lois « fourre-tout » nommées lois « pot-pourri », des mesures visant à simplifier, à améliorer, à clarifier ou à harmoniser les procédures existantes en matière d'administration de la justice. L'objectif visé est d'obtenir un meilleur fonctionnement de la justice (pour réduire la charge de travail des tribunaux), tout en concrétisant la poursuite de sa modernisation et de son informatisation. La C.P.V.P. a été amenée à se pencher, à plusieurs reprises, sur de nouveaux outils numériques supposés rendre l'administration de la justice plus efficace.

967 C.P.V.P., avis n° 28/2017 du 24 mai 2017, précité, n° 9.

968 *Ibid.*, n° 10.

969 *Ibid.*

970 Cette disposition pose que le consentement se dit de « toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement », ce qui ne correspond pas exactement à la définition du nouveau règlement européen, impliquant notamment un acte positif clair et univoque éventuellement posé électroniquement.

971 C.P.V.P., avis n° 28/2017, précité, n° 14.

972 *Ibid.*

973 Voy. *ibid.*

974 *Ibid.*, n° 17.

200. L'article 32*ter* du Code judiciaire. Cette disposition du Code a été insérée par la loi du 19 octobre 2015[975] (dite « loi pot-pourri I ») et modifiée ensuite par la loi du 25 décembre 2016[976] (dite « loi pot-pourri IV »). Elle prévoit que toutes les communications ou tous les dépôts intervenant entre les cours et tribunaux, le ministère public, les services qui dépendent du pouvoir judiciaire (greffes, …), les avocats, les huissiers et notaires peuvent se faire au « moyen du système informatique de la Justice désigné par le Roi ».

201. E-Box et e-Deposit. La Commission a rendu un avis sur le projet d'arrêté royal désignant deux systèmes informatiques auxquels il est possible de recourir dans le cadre de l'application de l'article 32*ter* précité, soit le système e-Box (pour les notifications, les communications et les dépôts) et e-Deposit (pour les dépôts de conclusions et pièces)[977]. L'avis est favorable, ces réseaux étant considérés par la C.P.V.P. comme permettant une communication plus efficace et plus moderne entre les acteurs du pouvoir judiciaire, mais cette dernière insiste sur le fait que la sécurité et la confidentialité des données doivent être assurées par la mise en place de techniques de cryptage lors de l'envoi de messages électroniques[978]. La Commission préconise également que des précisions soient apportées par l'arrêté royal au sujet de l'identité des responsables de traitement, des délais de conservation et sollicite que l'acte garantisse la mise en place d'un système de gestion et d'authentification des utilisateurs[979].

202. « Regsol ». Deux avis de la C.P.V.P. portent sur la création du « registre central de solvabilité » utilisé dans les procédures de faillites. La loi du 1er décembre 2016[980], en vigueur depuis le 1er avril 2017, a en effet modifié la loi du 8 août 1997 sur les faillites en y insérant ce registre, communément appelé « Regsol », qui constitue une base de données informatique dans laquelle le dossier de faillite est enregistré et conservé. La C.P.V.P. a examiné la proposition de loi à l'époque et a rendu un avis favorable sur celle-ci, ce pour autant que le législateur fournisse notamment une vision claire des catégories de données reprises dans le registre et envisage tant des sanctions applicables aux responsables de traitement qui méconnaitraient leurs obligations en matière de protection des données qu'un mécanisme de récupération des données par le SPF Justice au cas où les systèmes de gestion des données des responsables de traitement seraient défaillants[981]. Au travers d'un deuxième avis, la Commission rappelle qu'un comité de monitoring doit être mis en place au sein du SPF Justice avec pour objectif de veiller à la continuité des missions du service public liées au registre en cas de problèmes d'accès à la base de données sur le long terme[982].

975 Loi du 19 octobre 2015 modifiant le droit de la procédure civile et portant des dispositions diverses en matière de justice, *M.B.*, 22 octobre 2015.

976 Loi du 25 décembre 2016 modifiant le statut juridique des détenus et la surveillance des prisons et portant des dispositions diverses en matière de justice, *M.B.*, 30 décembre 2016.

977 C.P.V.P., avis n° 58/2015 du 16 décembre 2015 concernant un projet d'arrêté royal portant création de la communication électronique.

978 *Ibid.*, n° 15.

979 *Ibid.*, n° 12.

980 Loi du 1er décembre 2016 modifiant le Code judiciaire et la loi du 8 août 1997 en vue d'introduire le Registre central de la solvabilité, *M.B.*, 11 janvier 2017.

981 C.P.V.P., avis n° 35/2016 du 29 juin 2016 concernant la proposition de loi modifiant la loi du 8 août 1997 sur les faillites et introduisant le Registre central de la solvabilité, nos 15, 33 et 34.

982 C.P.V.P., avis n° 66/2016 du 19 décembre 2016 concernant l'arrêté royal organisant le fonctionnement du Registre central de la solvabilité, n° 6.

203. Registre central pour le recouvrement de dettes d'argent non contestées. La C.P.V.P. s'est aussi penchée sur le « registre central pour le recouvrement de dettes d'argent non contestées » au stade de l'avant-projet de la « loi pot-pourri I » et ensuite sur le projet d'arrêté royal portant exécution des nouvelles dispositions insérées par ladite loi dans le Code judiciaire (articles 1394/20 et suivants du Code judiciaire)[983]. Il s'agit d'un registre dans lequel les huissiers de justice encodent les exploits et procès-verbaux relatifs à la procédure de recouvrement de créances non contestées. La Commission rappelle que la finalité de la création de cette base de données est de permettre aux huissiers de consulter une copie de tous les exploits, citations, notifications, communications, … et que c'est seulement pour cette finalité que les huissiers peuvent consulter le registre. La Commission a en outre estimé qu'il convenait de préciser dans le texte de l'arrêté royal que l'identification des huissiers au moyen de leur carte *E-id.* visait à contrôler que ceux-ci n'outrepassaient pas leurs pouvoirs et également de veiller à ce que le responsable de traitement, à savoir la Chambre nationale des huissiers de justice, respecte les droits des citoyens (droit d'information, droit d'accès, droit de rectification et d'opposition et droit de ne pas être soumis à une décision automatisée)[984].

204. Les autres registres. Le « registre central des règlements collectifs de dettes », instauré lui aussi par la « loi pot-pourri IV » et le « registre central successoral », édifié par la loi du 6 juillet 2017 dite « loi pot-pourri V »[985], ont également fait l'objet d'avis de la C.P.V.P.[986]. Malgré l'émission de certaines remarques, des avis favorables ont été rendus par la Commission s'agissant de la création de ces nouveaux registres, dont le but est également de réduire les frais de justice et d'assurer un meilleur suivi des procédures.

b. La lutte contre la fraude sociale et/ou fiscale

205. Numérique au service des pouvoirs publics. L'usage croissant du numérique par les pouvoirs publics vise tantôt à favoriser l'efficacité des contrôles effectués sur les citoyens, tantôt à simplifier les formalités administratives. Les avis de la C.P.V.P. en matière de compteurs intelligents ainsi que de mises à jour du registre de la population offrent un intéressant éclairage à cet égard.

i. Les compteurs intelligents

206. Compteurs intelligents : des outils pour une consommation mieux maîtrisée et un contrôle de la fraude. Un compteur intelligent est un système de comptage numérique mesurant la consommation d'énergie et susceptible de communiquer cette consommation ainsi que d'autres informations aux gestionnaires de réseau de distribution. Dans la lignée de l'utilisation

983 C.P.V.P., avis n° 14/2015 du 13 mai 2015 au sujet de la création d'un registre central pour les créances non contestées et n° 11/2016 du 16 mars 2016 concernant le projet d'arrêté royal portant exécution du chapitre I*quinquies* du premier titre de la cinquième partie du Code judiciaire relatif au recouvrement de dettes d'argent non contestées.

984 C.P.V.P., avis n° 11/2016 du 16 mars 2016, précité, n^{os} 4-5 et avis n° 14/2015 du 13 mai 2015, précité, n^{os} 13 et 14.

985 Loi du 6 juillet 2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat et portant diverses mesures en matière de justice, *M.B.*, 24 juillet 2017.

986 C.P.V.P., avis n° 18/2016 du 27 avril 2016 au sujet de l'avant-projet de loi visant à créer un registre central des règlements collectifs de dettes ; C.P.V.P., avis n° 49/2016 du 21 septembre 2016 sur le projet de loi portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice.

croissante des *smart grid*s dits aussi réseaux intelligents[987] et sous l'impulsion européenne[988], ces compteurs permettent à la fois le stockage de différentes données de consommation ainsi que la commande à distance de certaines fonctionnalités du compteur comme l'ouverture, la fermeture, le prépaiement, etc.[989]. Ces outils sont également envisagés pour lutter contre la fraude sociale et/ou fiscale, plus particulièrement dans le cadre de l'abus d'adresses fictives, par le biais d'opérations de *datamining* ou exploration de données. Entre 2015 et 2017, la Commission se penche sur plusieurs demandes d'avis à ce sujet.

207. Échange de données en matière de lutte contre les adresses fictives. Au niveau fédéral, c'est sur un projet de loi visant à la transmission systématique de données de consommation des citoyens par les sociétés de distribution et gestionnaires de réseaux vers la BCSS, à dessein de contrôle des adresses fictives, que la Commission est amenée à se positionner[990]. La légitimité de la finalité du traitement de données personnelles relatives à la consommation d'énergie en vue de contrer la fraude au domicile est acceptée depuis 2012 déjà[991]. La réforme envisage l'instauration d'un système « push »[992], plus efficace, qui permet la transmission de données à caractère personnel en tant que « signal d'alerte à la fraude » dès lors qu'un écart de consommation de 80 % par rapport à la consommation moyenne est détecté en fonction de la composition du ménage telle qu'officiellement déclarée[993]. Constatant que son avis n° 24/2015 du 17 juin 2015 n'a pas été entièrement suivi, la Commission prend une décision partiellement favorable sur plusieurs pans du projet en l'état. Ainsi, elle pointe du doigt l'encadrement légal du *datamining*, qui devrait être consacré dans un texte de valeur législative[994], comme en matière de traitement de données à caractère personnel par le Service public fédéral Finances[995]. Elle poursuit en insistant sur la nécessaire désignation du responsable de traitement, à plus forte raison au vu de la multiplicité des acteurs engagés dans le processus[996], et sur celle du *data protection officer*, découlant de la nouvelle réglementation européenne[997]. Elle précise ensuite qu'un délai adapté de conservation

987 Sur le sujet, voy. C.P.V.P., recommandation n° 04/2011 du 25 juin 2011 quant aux principes à respecter pour les smart grids et les compteurs intelligents.

988 Voy. recommandation 2012/148/UE de la Commission européenne du 9 mars 2012 relative à la préparation de l'introduction des systèmes intelligents de mesure, *J.O.U.E.* L 73/9 du 13 mars 2012.

989 Voy. notamment le site d'ORES à ce sujet : https://www.ores.be/particuliers-et-professionnels/smart-metering.

990 Voy. C.P.V.P., avis n° 05/2016 du 3 février 2016 concernant le projet de loi modifiant la loi-programme sur le contrôle de l'abus d'adresses fictives par les bénéficiaires des prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation des sociétés de distribution et des gestionnaires de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale ainsi que l'avis précédent : C.P.V.P., avis n° 24/2015 du 17 juin 2015 concernant le chapitre II du projet de loi portant des dispositions diverses, relatif aux données de consommation des sociétés de distribution et des gestionnaires de réseaux de distribution.

991 Voy. C.P.V.P., avis n° 06/2012 du 8 février 2012 relatif à l'avant-projet de loi-programme en ce qui concerne la lutte contre la fraude et plus particulièrement le contrôle sur l'abus des adresses fictives par les assurés sociaux, n° 10.

992 Projet de loi modifiant la loi-programme du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires des prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation des sociétés de distribution et des gestionnaires de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale, *Doc. parl.*, sess. 2015-2016, n° 1554/001, p. 8, al. 2.

993 C.P.V.P., avis n° 05/2016 du 3 février 2016, précité, n° 8.

994 *Ibid.*, n° 15.

995 Voy. art. 5, § 1er, 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, *M.B.*, 24 août 2012.

996 C.P.V.P., avis n° 05/2016 du 3 février 2016, précité, n° 16.

997 Art. 35-37 du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité.

des données doit être précisé, bien qu'« il est évident que les données ne sont conservées par la BCSS que pendant le temps nécessaire au couplage des données et à leur transmission aux institutions de sécurité sociale concernées »[998]. En ce qui concerne la transparence et les droits d'accès et de rectification des personnes concernées, la Commission s'oppose à ce que l'inspection sociale puisse se prévaloir du mécanisme d'exception prévu dans le cas de missions de police administrative au sens du Code pénal social, arguant « qu'il ne s'agit finalement que de données d'utilisateurs, ni plus ni moins »[999]. Enfin, elle déplore l'absence de droits supplémentaires des personnes concernées à l'égard des actes d'investigation effectués suite à un « signal d'alerte à la fraude », comme la possibilité de s'opposer à la sélection par des techniques de *datamining* et l'instauration de rapports d'actes d'investigation par l'inspection sociale[1000]. Notons que c'est une loi du 13 mai 2016[1001] qui vient entériner ces changements.

208. Échange de données en matière de lutte contre la fraude à l'énergie. En Flandre, c'est un projet de modification du décret sur l'énergie de 2009 en ce qui concerne la prévention, la détection, la constatation et la sanction de la fraude à l'énergie[1002] ainsi qu'une note sur le déploiement des compteurs numériques[1003] qui retiennent l'attention de la Commission. La réforme tend à imposer aux gestionnaires de réseaux de distribution une obligation de rechercher et prévenir activement les formes de fraude à l'énergie[1004]. Toutes les données auxquelles ces derniers ont accès peuvent être utilisées et d'importants pouvoirs d'investigation et de constatation leur sont dévolus[1005]. Rappelant que la base décrétale « constitue une exigence minimale mais n'est en soi pas suffisante pour légitimer toutes les immixtions possibles »[1006], la Commission pose les exigences du principe de légalité. Ainsi, elle recommande un « ancrage légal » pour le responsable de traitement, la nature du traitement, les catégories de données traitées, le groupe de population visé et le délai de conservation des données[1007]. Plus fondamentalement encore, pour elle, « la surveillance continue du comportement énergétique de tous les utilisateurs flamands (personnes physiques) d'électricité (ménages, PME) […] ne peut pas être considérée comme une mesure nécessaire dans une société démocratique afin de poursuivre une finalité légitime (la lutte contre la fraude) »[1008]. Des garanties, notamment en termes de transparence ou d'accès et de recti-

998 C.P.V.P., avis n° 05/2016 du 3 février 2016, précité, n° 20.

999 *Ibid.*, n° 27.

1000 C.P.V.P., avis n° 24/2015 du 17 juin 2015, précité, n°s 39 à 45.

1001 Loi du 13 mai 2016 modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale, *M.B.*, 27 mai 2016.

1002 C.P.V.P., avis n° 25/2016 du 8 juin 2016 relatif au projet de décret modifiant le décret sur l'énergie du 8 mai 2009, en ce qui concerne la prévention, la détection, la constatation et la sanction de la fraude à l'énergie ainsi que l'avis suivant : C.P.V.P., avis n° 47/2017 du 20 septembre 2017 relatif au projet d'arrêté du Gouvernement flamand modifiant l'arrêté relatif à l'énergie du 19 novembre 2010 en ce qui concerne la prévention, la détection, la constatation et la sanction de la fraude à l'énergie.

1003 C.P.V.P., avis n° 17/2017 du 12 avril 2017 sur un projet de note « *uitrol van digitale meters in Vlaanderen* » du ministre flamand du Budget, des Finances et de l'Énergie.

1004 C.P.V.P., avis n° 25/2016 du 8 juin 2016, précité, n° 5.

1005 Voy. *ibid.*, n°s 6-8.

1006 *Ibid.*, n° 13.

1007 *Ibid.*, n°s 17 à 24.

1008 *Ibid.*, n° 26.

fication, doivent encadrer les techniques de profilage utilisées. L'avis rendu sur le projet de modification du décret est donc défavorable en ce qu'il constate une violation des principes de légalité et de proportionnalité. De plus, l'avis relatif au projet d'arrêté de Gouvernement évoque des « réserves quant au fait que la même instance […] et/ou les mêmes personnes puissent réaliser une exploration de données, créer et tester des modèles de profilage, réaliser des enquêtes et infliger des sanctions […] avec suffisamment de garanties en matière d'expertise, d'indépendance et d'impartialité »[1009]. L'examen du projet de note « *uitrol van digitale meters in Vlaanderen* » par la Commission révèle lui aussi plusieurs faiblesses. D'abord, divers éléments essentiels doivent être traités par le décret et non pas laissés au Gouvernement. Il en va ainsi notamment des catégories de données traitées et des finalités d'utilisation[1010]. Ensuite, la conformité avec le RGPD doit être soignée, surtout au niveau des droits de la personne concernée vis-à-vis de ses données personnelles[1011]. Partant, une distinction nette doit être faite entre l'obligation d'installation et le consentement à toutes les fonctionnalités du compteur intelligent[1012].

209. Compteurs intelligents. La Commission se tourne également vers le marché du gaz et de l'électricité en Région de Bruxelles-Capitale. En effet, un avant-projet d'ordonnance anticipant le développement des compteurs intelligents lui est soumis début juillet 2017[1013]. À cette occasion, elle est amenée à enjoindre la ministre de rechercher la concertation avec les autres Communautés en vue d'établir une protection des données à caractère personnel homogène sur tout le territoire[1014]. Elle souligne également que la possibilité laissée au gestionnaire de réseau de distribution de déléguer certaines tâches ne l'exempte pas de ses obligations de responsable de traitement. En vertu de la réglementation européenne, il est chargé spécialement du respect des droits de la personne concernée, de la tenue d'un registre des activités de traitement ou encore de mener une analyse d'impact[1015].

ii. *La mise à jour du registre de la population*

210. Modifications au service de la lutte contre la fraude au domicile et une certaine fraude sociale ou fiscale. Le 12 octobre 2016, la C.P.V.P. rend un avis favorable sur un projet d'arrêté royal modifiant plusieurs arrêtés royaux relatifs aux registres de la population et aux cartes d'identité, ce pour clarifier ou simplifier les réglementations existantes et pour participer à l'objectif du Gouvernement[1016]. La C.P.V.P. évalue plusieurs modifications apportées par le projet d'arrêté royal, comme par exemple l'obligation de procéder à une enquête lorsque quelqu'un souhaite fixer sa résidence dans une commune ou encore la collaboration avec les fournisseurs d'énergie ou de télécoms pour obtenir les données de consommation des citoyens. La Commission a considéré que ces deux modifications étaient proportionnées aux finalités recherchées (lutte contre les

1009 C.P.V.P., avis n° 47/2017 du 20 septembre 2017, précité, n° 29.
1010 C.P.V.P., avis n° 17/2017 du 12 avril 2017, précité, n° 12.
1011 *Ibid.*, n^os 47-49.
1012 *Ibid.*, n^os 40-46.
1013 C.P.V.P., avis n° 35/2017 du 5 juillet 2017.
1014 *Ibid.*, n° 19.
1015 *Ibid.*, n° 29.
1016 C.P.V.P., avis n° 55/2016 du 12 octobre 2016 sur le projet d'arrêté royal modifiant l'arrêté royal du 16 juillet 1992 déterminant les informations mentionnées dans les registres de la population et dans le registre des étrangers ainsi que d'autres arrêtés royaux.

domiciliations fictives et les fraudes sociales ou fiscales), en rappelant néanmoins que les vérifications auprès des fournisseurs précités ne devaient intervenir que si d'autres moyens moins intrusifs comme les visites sur place ou les demandes de convocation étaient restés infructueux[1017].

c. La consultation des données de la DIV

211. Nécessité d'une autorisation du comité sectoriel. Par un arrêt rendu le 13 décembre 2016, la Cour de cassation a estimé que, bien que la recherche et la constatation des infractions de roulage ressortent des missions de la police, cela n'implique pas que la police puisse identifier le titulaire d'une plaque d'immatriculation via la DIV sans avoir l'autorisation du comité sectoriel de la C.P.V.P. d'accéder aux données à caractère personnel de la Banque-Carrefour des véhicules[1018]. La police fédérale a aujourd'hui régularisé la situation étant donné que, suite à une demande qui lui a été soumise le 15 décembre 2016, soit quelques jours après l'arrêt de la Cour, le comité sectoriel pour l'Autorité fédérale a autorisé la communication des données à caractère personnel (données relatives à la plaque d'immatriculation, données relatives au véhicule, données relatives au titulaire du véhicule et données relatives au conducteur habituel du véhicule) de la DIV vers les services de police[1019].

d. Le dossier social électronique partagé

212. Un projet de dossier social informatisé unique et centralisé pour les personnes sans-abri. Fin mai 2017, la Commission se prononce sur une demande d'avis relative à un projet d'ordonnance en matière d'aide d'urgence et d'insertion des personnes sans-abri en Région de Bruxelles-Capitale[1020]. Saisie par les membres du collège réuni de la Commission communautaire commune, elle se penche plus particulièrement sur les dispositions portant création d'un dossier social électronique reprenant les données personnelles (comprenant notamment données d'identification, historique du parcours de vie et d'aide sociale, etc.) des plus précarisés[1021]. Le projet d'ordonnance a pour objectif d'« imposer à chaque centre de collaborer à l'établissement d'un dossier social informatisé unique et centralisé pour chaque usager, et de collaborer au partage des données y relatives »[1022]. Les données récoltées par les travailleurs sociaux seront intégrées à un « réseau des dossiers sociaux », en vue de leur partage ultérieur avec les centres d'aide, et structurées autour de deux organes coordinateurs, un pour l'aide d'urgence et un pour l'aide d'insertion. Une ASBL

1017 *Ibid.*, n° 20.

1018 Cass. (2e ch. N), 13 décembre 2016, R.G. n° P.16.0682.N, note E. Degrave, « PV pour excès de vitesse : les services de police peuvent-ils accéder librement aux données de la DIV ? », *R.D.T.I.*, 2016, n° 65, pp. 63 à 71.

1019 Comité sectoriel pour l'Autorité fédérale, Délibération AF n° 53/2016 du 15 décembre 2016 relative à la demande d'autorisation de la Direction de l'information policière et des moyens ICT (DRI) de la Police Fédérale de communication électronique de données de la DIV nécessaires à la police intégrée afin d'exercer ses missions de police judiciaire et administrative.

1020 C.P.V.P., avis n° 25/2017 du 24 mai 2017 concernant une demande des membres du collège réuni de la Commission communautaire commune de Bruxelles-Capitale, compétents pour l'aide aux personnes, à propos d'un projet d'ordonnance relative à l'aide d'urgence et à l'insertion des personnes sans-abri.

1021 Sur le modèle du rapport social électronique tel qu'implémenté au sein des CPAS par la circulaire ministérielle du SPP Intégration sociale du 23 décembre 2015 concernant la mise en production du rapport social électronique, disponible sur : https://www.mi-is.be/fr/reglementations/circulaire-concernant-la-mise-en-production-du-rapport-social-electronique.

1022 C.P.V.P., avis n° 25/2017 du 24 mai 2017, précité, n° 5.

« Bureau d'insertion sociale » se charge de la centralisation de ces dossiers, ainsi que de la gestion de la sécurisation et du traitement desdites informations[1023].

La Commission émet plusieurs recommandations à l'égard du projet.

Premièrement, elle insiste sur la nécessité de désigner un intégrateur de services. Si le Bureau d'insertion sociale est responsable du stockage, de la sécurisation et du traitement des données, il est aussi chargé de l'accès à celles-ci par les centres et l'opérateur coordinateur de l'aide urgente. Dans cette optique, la Commission suggère de nommer un tiers de confiance – à l'instar de l'intégrateur de services bruxellois – et/ou de recourir à l'ordonnance du Parlement de la Région de Bruxelles-Capitale du 8 mai 2014[1024], afin d'« assurer que les garanties requises sont en place pour le partage de données envisagé »[1025]. Il est question à la fois d'empêcher les conflits d'intérêts, de respecter les conditions du secret professionnel partagé dans le cadre de l'échange de données, tout en remplissant la fonction d'analyse statistique.

Deuxièmement, la Commission invite à clarifier la désignation et les responsabilités du responsable de traitement. Ainsi, le projet d'ordonnance prévoit la responsabilité du Bureau d'insertion sociale en matière de partage des dossiers sociaux[1026]. Cet état des choses « vise à tout le moins à retirer aux acteurs de terrain, en tout ou en partie, leur pouvoir de décision concernant les finalités et moyens de traitement »[1027]. Il convient donc se référer à la recommandation précédente pour pallier cet écueil, tout en attachant une importance toute particulière à la disponibilité et au partage de l'information dans la mesure où elle est nécessaire à l'accomplissement des missions des travailleurs sociaux[1028].

Dans un troisième temps, la Commission enjoint de limiter les accès aux données du Bureau conformément à ses missions, pointant du doigt un accès « général » et « excessif »[1029], tel que prévu dans le projet. Dans ce sens, il est notamment indispensable de créer une liste de données via des critères permettant d'établir s'il s'agit d'informations nécessaires à l'exercice des fonctions (comme la coordination de l'aide d'insertion)[1030].

Quatrièmement, le respect des conditions de partage du secret professionnel est abordé. Les informations contenues dans les dossiers sociaux électroniques sont couvertes par le secret professionnel[1031]. Sachant qu'il préserve aussi bien les intérêts de la personne en situation de besoin « afin que les informations qu'elle a confiées fassent l'objet de la plus grande confidentialité », que ceux de la société « afin de pouvoir en toute confiance recourir aux services de certains groupes cibles », comme les médecins ou assistants sociaux[1032], le secret professionnel ne peut être partagé que sous certaines conditions. Cette pratique de terrain, non encadrée légalement, doit, selon la Commission, se plier à plusieurs exigences : information de la personne concernée par le partage

1023 *Ibid.*, nos 6 et 7.
1024 *Ibid.*, nos 14 et 15.
1025 *Ibid.*, no 16.
1026 Voy. *ibid.*, no 22.
1027 *Ibid.*
1028 Voy. *ibid.*, no 24.
1029 *Ibid.*, no 25.
1030 *Ibid.*, nos 25-26.
1031 *Ibid.*, no 29.
1032 *Ibid.*, no 31.

d'informations et consentement préalable de celle-ci (i), nécessité du partage de données dans l'intérêt de la personne (ii), transfert de données uniquement entre professionnels tenus par le secret et exerçant une activité identique (iii), transmission des informations nécessaires et utiles uniquement (iv), et ce, de manière sécurisée (v)[1033]. Relativement au consentement de la personne concernée par le partage, la faculté de refuser la collecte de ses données ou de s'opposer à leur traitement inscrite dans le projet se rapproche d'un « opt-out », « et non un consentement préalable au sens de la LVP »[1034]. Or, au vu des données contenues dans le dossier, il s'agit d'instaurer une obligation renforcée de consentement préalable, comme en matière de partage de données médicales[1035]. En ce qui concerne la sécurisation des données, la C.P.V.P. souligne le manque de précision du projet quant aux rôles attachés au délégué à la protection des données et souligne que « les fonctions assumées par le conseiller en sécurité de l'information d'une part, et le préposé à la protection des données d'autre part sont différentes »[1036]. Finalement, d'autres obligations en matière de vie privée sont évaluées, pour parvenir à un avis partiellement défavorable jugeant la responsabilité du Bureau d'insertion sociale, en lieu et place d'un intégrateur de service, dans le cadre d'un dossier social unique et centralisé pour tout bénéficiaire d'aide contraire aux dispositions applicables en matière de protection de la vie privée[1037].

IV. MÉDIAS, LIBERTÉ D'EXPRESSION ET NOUVELLES TECHNOLOGIES

Quentin Van Enis[1038] et Alejandra Michel[1039]

213. Introduction et plan de la contribution. La présente section vise à rendre compte des principales décisions rendues par les cours et tribunaux de 2015 à 2017. À côté de ces décisions judiciaires à strictement parler, il nous a paru intéressant de présenter certains développements issus de la « jurisprudence » du Conseil de déontologie journalistique (« CDJ »), organe d'autorégulation compétent pour les activités journalistiques des médias belges d'expression francophone et germanophone[1040]. Ce choix est notamment dicté par la tendance croissante[1041] des juges, nationaux et internationaux, à faire reposer leur raisonnement sur les enseignements de la déontologie journalistique, principalement en ce qui concerne l'examen du comportement du

1033 Voy. *ibid.*, n° 33.

1034 *Ibid.*, n° 36.

1035 *Ibid.*

1036 *Ibid.*, n° 47. Voy. aussi : https://www.privacycommission.be/fr/faq-themas/d%C3%A9l%C3%A9gu%C3%A9-%C3%A0-la-protection-des-donn%C3%A9es.

1037 Elle émet cependant un avis favorable quant à la mise en disposition et au partage des données personnelles relatives au bénéficiaire d'aide, sous certaines réserves.

1038 Chargé de cours invité à l'UNamur (CRIDS), membre du Conseil de Déontologie Journalistique.

1039 Chercheuse au CRIDS (UNamur) et membre du NADI.

1040 Deux observations méritent d'être formulées quant au champ d'action du CDJ. D'une part, le CDJ s'estime compétent pour l'ensemble des supports de diffusion d'information (presse écrite, audiovisuelle ou numérique). D'autre part, pour définir sa compétence, le CDJ prend pour critère déterminant le « fait de diffuser de l'information de type journalistique vers le public ». Il étend ainsi sa compétence à toute activité de nature journalistique, que la personne exerçant une telle activité soit ou non un professionnel du journalisme ou un membre d'une association professionnelle. Sur ce point, voy. CDJ, « Champs d'action du CDJ », disponible sur http://lecdj.be/la-deontologie/champs-daction-du-cdj/.

1041 Voy. déjà notre précédente chronique, Q. Van Enis, « Droit des médias, liberté d'expression et nouvelles technologies (chronique de jurisprudence 2012-2014) », *R.D.T.I.*, 2015, p. 182, n° 331.