contracter[350]. En l'espèce, DNS BE n'avait pas respecté son règlement d'enregistrement en accordant un nom de domaine à une asbl qui n'était pas encore juridiquement constituée (alors que les règles en vigueur à cette époque ne le permettaient pas) et en refusant par conséquent le même nom de domaine à un demandeur ultérieur qui était lui dans les conditions prescrites par les règles de DNS BE. Bien que la cour considère la faute de DNS BE comme établie, elle condamne seulement cette dernière à réparer le dommage moral du demandeur évincé, ce qui est pour le moins symbolique et ne permet pas de récupérer le nom de domaine convoité.

3. Noms commerciaux et métatags

96. Usage d'un nom commercial dans un métatag. Aucune décision majeure n'est à relever au cours de la période sous revue.

Tout au plus, observera-t-on la confirmation que l'usage du nom commercial d'un concurrent dans les métatags d'un site web constitue un acte contraire aux usages honnêtes en matière commerciale[351]. Cette jurisprudence devrait cependant être relue à la lumière des récents arrêts de la Cour de justice en matière de responsabilité des annonceurs pour atteinte au droit des marques. Le raisonnement de la Cour à cet égard nous paraît en effet transposable à la protection des noms commerciaux.

III. LIBERTÉS ET SOCIÉTÉ DE L'INFORMATION

Coordination par Jean-Marc Van Gyseghem[352]

A. Vie privée et protection des données à caractère personnel

1. Juridictions judiciaires[353] (Sandrine Hallemans et Maïté Van Winckel)[354] *et constitutionnelle* (Jean-Marc Van Gyseghem)

97. Introduction. Il n'y a pas lieu de s'attarder dans cette chronique sur l'ensemble des décisions belges concernant les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme. On ne relèvera que les décisions relatives à des situations faisant intervenir d'une façon ou d'une autre les technologies de l'information et de la communication. Concernant l'article 8 C.E.D.H., il est à remarquer que le droit fondamental consacré par cet article est régulièrement appliqué par les tribunaux de manière horizontale, c'est-à-dire qu'il doit être respecté aussi bien par les pouvoirs publics que par les particuliers vis-à-vis d'autres particuliers[355].

98. L'article 22 au regard des normes internationales. Dans son arrêt du 18 mars 2010, la Cour constitutionnelle a considéré que : « (…) La Cour peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de la directive précitée

350 Bruxelles, 20 octobre 2011, R.G. n° 2007/AR/2611, inédit, disponible sur http://www.darts-ip.com.

351 Comm. Namur, 3 mars 2010, *R.D.T.I.*, 2010, p. 151.

352 Directeur de l'Unité de recherche « Libertés et société de l'information » du CRIDS (www.crids.eu) et avocat au barreau de Bruxelles (www.rawlingsgiles.be).

353 Les auteures remercient la professeure de Terwangne pour la relecture attentive qu'elle a effectuée.

354 Chercheuses au CRIDS (www.crids.eu).

355 F. Sudre, *Droit européen et international des droits de l'homme*, 8e éd., Paris, PUF, 2006, n° 141.

[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] et de la convention n° 108 [du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel] auxquelles la loi précitée du 8 décembre 1992 [relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel] et ses modifications ultérieures donnent exécution. *Ces obligations forment un ensemble indissociable des garanties qui sont reproduites à l'article 22 de la Constitution* »[356]. Ainsi, la Cour réaffirme la filiation de l'article 22 de la Constitution avec les normes internationales qui sous-tendent le droit à la protection de la vie privée. Cela donne également une clef d'analyse de cet article 22 dès lors que les interprétations de l'article 8 de la Convention européenne des droits de l'homme rendues par la Cour européenne des droits de l'homme de Strasbourg lui sont applicables. Cela a été confirmé une nouvelle fois, en d'autres termes, par la Cour qui a considéré qu'« il ressort des travaux préparatoires de [l'] article [22] que le Constituant [a] cherché à mettre le plus possible la proposition en concordance avec l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (C.E.D.H.), afin d'éviter toute contestation sur le contenu respectif de l'article de la Constitution et de l'article 8 de la C.E.D.H. (*Doc. parl.*, Chambre, 1993-1994, n° 997/5, p. 2) »[357].

99. Droit au respect de la vie privée[358]**.** La cour d'appel de Gand a jugé que l'enregistrement et l'impression d'extraits de la mémoire de l'ordinateur personnel d'un enfant mineur par un de ses parents, en son absence et sans son autorisation préalable, constituent une violation du droit au respect de la vie privée protégé par l'article 8 de la Convention européenne des droits de l'homme. Le degré de cette violation sera d'autant plus important que l'enfant approchera de la majorité[359].

Également en matière de surveillance, mais émanant cette fois-ci des autorités publiques, lors d'une information pénale, le parquet avait procédé, entre autres, à des écoutes et prises de connaissance de SMS entrants et sortants pour une période donnée. À la question de savoir s'il y avait atteinte au droit au respect de la vie privée, il a été décidé que ces mesures étaient gravement attentatoires à la vie privée et que seules des circonstances exceptionnelles[360] pouvaient justifier leur mise en œuvre[361].

Cependant, tout enregistrement d'une conversation téléphonique ne peut être exclu sous couvert du droit au respect de la vie privée, comme cela a été jugé par la cour d'appel de Gand le 16 février 2010[362]. Après avoir mis en balance le droit de la preuve et le droit au respect de la vie privée, la Cour n'a pu toutefois admettre que seul l'enregistrement d'une conversation télé-

356 Cour const., 18 mars 2010, 29/2010, www.const-court.be ; nous soulignons.

357 Cour const., 10 novembre 2011, 166/2011, www.const-court.be, B.16.6. Voy. également Cour const., 7 juillet 2011, (122/2011), www.const-court.be, B.3.

358 Le point 107 traite aussi dans une certaine mesure de la question du droit au respect de la vie privée protégé par les articles 22 et 8.

359 Gand, 23 avril 2009, *R.A.B.G.*, 2010/12, p. 807.

360 Voy. à l'article 90*ter* du Code d'instruction criminelle pour une énumération de circonstances exceptionnelles autorisant les écoutes téléphoniques.

361 Liège (20e ch.), 3 décembre 2009, *J.T.*, 12/2010, pp. 192-193.

362 Gand (14e ch.), 16 février 2010, *T.G.R.*, 2010, p. 258.

phonique privée entre deux ex-époux pouvait apporter des éléments nécessaires à la preuve de paiements faits en exécution d'une convention conclue après divorce.

Dans une affaire de contrôle systématique des sacs des spectateurs avant un concert, le tribunal civil de Bruxelles a jugé que ce type de contrôle méconnaît à la fois « la loi du 10 avril 1990, mais aussi les règles les plus élémentaires de l'État de droit, [tel que] le respect de la vie privée (…) »[363].

Le juge de paix de Roulers a eu à se prononcer sur une demande d'informations d'un propriétaire auprès du receveur de l'enregistrement. Il s'agissait d'une demande de renseignements concernant la superficie, le revenu cadastral, le prix de location, etc. des biens immobiliers avoisinant le bien du requérant. Une mise en balance doit être réalisée entre deux droits fondamentaux : le droit à la vie privée des propriétaires voisins sur la base de l'article 22 de la Constitution et le droit à l'information du demandeur, ce droit étant avancé par le juge sans autre précision. Le juge a conclu que d'autres moyens pourraient être déployés par le demandeur pour obtenir de telles informations, la mesure requise étant dès lors disproportionnée.

Le fait pour des enquêteurs d'apprendre de la part d'un opérateur téléphonique que des numéros de téléphone dont ils connaissent les titulaires sont ou non actifs, n'est pas une information concernant la vie privée et ne constitue dès lors pas une violation de celle-ci en vertu des articles 8 de la Convention européenne des droits de l'homme et 22 de la Constitution[364].

Enfin, nous pouvons relever que le droit au respect de la vie privée « bénéficie aussi, dans une certaine mesure, aux personnes morales. Dès lors, il peut être admis que le droit au respect de la vie privée des personnes morales englobe la protection de leurs secrets d'affaires »[365]. Ici également, ce sera au juge de procéder à une balance des intérêts en présence, en l'occurrence le droit au respect de la vie privée et le droit à un procès équitable. Lorsque des documents indispensables au bon déroulement d'un procès ne sont pas communiqués à la partie adverse, le droit à un procès équitable est, en principe, violé. « (…) [C]e principe doit céder lorsque son application stricte engendrerait une violation manifeste du droit au respect de la vie privée de certaines personnes, en leur faisant courir un risque particulièrement grave et très difficilement réparable »[366].

100. Données à caractère personnel au sens de l'article 1er, § 1er, de la L.V.P.[367] Une donnée à caractère personnel est une donnée relative à une personne physique identifiée ou identifiable[368].

C'est ainsi qu'il a été jugé par la cour d'appel de Liège que l'identité des membres d'un forum ainsi que leurs données de connexion sont constitutives de données à caractère personnel au sens de la L.V.P.[369] Une adresse IP ou un log ont été considérés comme des données à caractère personnel. Dans ce litige qui concernait des propos tenus sur un forum de discussion, l'entreprise en cause avait demandé à Test-Achats de produire « les informations en sa possession concernant l'iden-

363 Civ. Bruxelles (9e ch.), 26 février 2009, *J.L.M.B.*, 2010/10, 461.
364 Cass., 26 mai 2009, www.cass.be.
365 Bruxelles (9e ch.), 30 juin 2010, *J.L.M.B.*, 2011/25, p. 1184.
366 Bruxelles (9e ch.), 30 juin 2010, *J.L.M.B.*, 2011/25, p. 1184.
367 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
368 Article 1er, § 1er, de la L.V.P.
369 Liège (7e ch.), 22 octobre 2009, *R.D.T.I.*, n° 38/2010, pp. 95 et s.

tité, les coordonnées, les adresses TCP/IP et les logs des auteurs des messages litigieux (…) ». Elle basait sa demande d'information sur l'article 21 de la loi du 11 mars 2003. Après que Test-Achats se fut exécuté, l'une des personnes dont l'identité a été révélée grâce à son adresse IP a contesté avoir accédé au forum et a déposé plainte pour usurpation de son numéro d'identification de membre de Test-Achats.

Dans un arrêt rendu quelques jours plus tard, la même cour d'appel de Liège a indiqué que les adresses électroniques des personnes contactées dans le cadre d'une pratique de marketing viral, c'est-à-dire l'envoi automatique de courriels publicitaires sans autorisation, constituaient des données à caractère personnel[370].

La Cour de cassation, dans un arrêt du 26 mai 2009, a précisé que s'agissant des données relatives aux informations quant aux échanges téléphoniques ou aux éléments d'appel, elles sont également qualifiées de données à caractère personnel[371].

101. Données sensibles. La L.V.P. prévoit un régime plus protecteur pour certains types de données : les données sensibles parmi lesquelles on retrouve les données qui révèlent les opinions politiques et les données judiciaires.

Le 17 mars 2010, la cour d'appel de Bruxelles a été saisie d'une affaire concernant une personne qui avait reçu de nombreux mails du Front National. En effet, ce parti extrémiste avait établi une *mailing list* dans laquelle l'adresse mail de cet individu apparaissait. Ce fichier n'était pas exclusivement constitué d'adresses de membres ou de partisans du Front National, il comprenait entre autres des adresses mail appartenant à des personnes qui n'adhéraient indubitablement pas aux opinions promues par ce parti. Selon la cour, « le fichier dans lequel figurait la partie civile n'était pas de nature à révéler, en particulier, les opinions politiques de la partie civile, dès lors qu'il n'était pas destiné à répertorier les membres ou les sympathisants du parti Front National mais bien les personnes physiques ou morales souhaitant être informées des activités du parti, par intérêt professionnel, par sympathie ou même par simple curiosité »[372].

Une autre affaire opposait des employés communaux à la RTBF et concernait la diffusion, lors d'un J.T., d'images de ces employés distribuant des tracts électoraux[373]. Les demanderesses ont allégué la violation des articles 4, 5 et 6, § 1er, de la L.V.P. et de l'article 8 de la Convention européenne des droits de l'homme. Elles ne contestaient par ailleurs pas avoir distribué des tracts électoraux sur un marché. Au cours de cette affaire s'est posée la question du rapport entre la protection des opinions politiques manifestées dans la sphère privée et l'exercice de cette liberté d'opinion dans la sphère publique. Le tribunal va dire que « contrairement à ce qu'allèguent les demanderesses, il n'existe toutefois aucun rapport entre la protection des opinions politiques manifestées dans la sphère privée, qui est régie par les dispositions invoquées par les demanderesses et l'exercice de cette liberté d'opinion dans la sphère publique, comme ce fut le cas en l'espèce ». Le tribunal a donc estimé que la première est soumise à la L.V.P. tandis que les dispositions de la L.V.P. ne

370 Liège (7e ch.), 19 novembre 2009, *D.A. O.R.*, 2010/96, p. 453. Nous analyserons plus en détail cette décision *infra*.
371 Cass., 26 mai 2009, www.cass.be.
372 Bruxelles (11e ch. corr.), 17 mars 2010, *R.D.T.I.*, no 42/2011, p. 53.
373 Civ. Bruxelles (14e ch.), 9 juin 2009, *A&M*, 2010/1, pp. 106 et s.

sont pas applicables à la seconde[374]. Le tribunal a, ainsi, cru nécessaire de se placer au niveau de la distinction qui existe entre la sphère publique et la sphère privée, alors que cela n'est pas prévu par la L.V.P. Il a fait une analyse erronée qui ne peut être suivie, car en effet, la L.V.P. n'est pas limitée à une sphère particulière, il suffit que l'on se trouve en présence de traitement de données à caractère personnel. On peut se poser la question de savoir si ce n'est pas une référence uniquement à l'article 8 de la Convention européenne des droits de l'homme qui a été faite par le juge, en oubliant les dispositions de la L.V.P. également invoquées. Si c'est le cas, la distinction faite par le juge entre sphères privée et publique est effectivement pertinente.

Conformément à la loi du 8 décembre 1992, un employeur ne peut exiger d'un travailleur qu'il produise un certificat de bonne vie et mœurs[375]. Le tribunal dans l'affaire dont question ici va se baser sur un article de doctrine dans lequel il est précisé que, concernant le traitement des données judiciaires, aucune base légale n'autorise explicitement le contrôle par un employeur des antécédents judiciaires d'un employé, sous réserve de deux exceptions : la première permet la récolte et la conservation du certificat de bonne vie et mœurs si la profession l'exige, la seconde permet la simple prise de connaissance du contenu – la lecture d'un document – à condition que la personne concernée ait donné son consentement[376]. Il est regrettable que le tribunal n'ait pas plus justifié son raisonnement dès lors que le consentement en présence de données sensibles n'est pas valable dans les liens du travail. Le tribunal a également rajouté que la L.V.P. interdit la conservation de certificats de bonne vie et mœurs.

102. Traitement des données à caractère personnel. Un traitement de données est défini dans la loi vie privée comme étant « 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 »[377]. Cette notion a été définie largement, ce qui permet aisément d'y faire entrer diverses situations, telles celles des détectives privés, du spam et du marketing viral.

En matière de marketing viral, il existe deux manières principales de procéder. L'organisation de la première repose sur l'éditeur du site : une page internet invite les internautes inscrits à communiquer les adresses mail de leurs connaissances et c'est alors le site qui génère l'envoi du mail à ces personnes. La seconde méthode repose sur les internautes eux-mêmes : le site propose aux internautes inscrits un mail-type qu'ils pourront ensuite de leur propre initiative envoyer à leurs connaissances. Cette façon de procéder n'implique aucune communication de données à caractère personnel à l'éditeur du site. Par opposition, la première méthode de marketing viral conduit à communiquer des adresses mail à l'éditeur du site qui a alors « entière maîtrise des moyens mis

374 Civ. Bruxelles (14e ch.), 9 juin 2009, *A&M*, 2010/1, p. 113.
375 Comm. Charleroi (2e ch.), 17 décembre 2009, *J.T.T.*, 2010, pp. 398-399.
376 R. De Baerdemaecker, « Protection de la vie privée et contrat de travail », *J.T.T.*, 2006, pp. 1-13.
377 Article 1er, § 2 de la L.V.P.

en œuvre pour le traitement de ces données », dans le respect, toutefois, des conditions que la L.V.P. impose. Dans cette matière, la cour d'appel de Liège s'est prononcée le 19 novembre 2009[378]. « Nice people » est un site de rencontres qui a pour pratique de collecter les adresses mail des contacts de ses utilisateurs pour proposer par mail à ces derniers de venir découvrir le site en question. « Toi et moi », site de rencontres concurrent, conteste les méthodes utilisées par « Nice People » pour augmenter le nombre de ses utilisateurs, méthodes qu'elle juge contraires notamment à la L.V.P. et plus précisément aux règles applicables au traitement des données à caractère personnel. Le marketing viral est un traitement de données à caractère personnel. Même si « Nice people » conteste l'existence d'un traitement au sens de la loi car selon elle il n'y aurait qu'une simple consultation des données, la cour va considérer que le fait que les données collectées soient automatiquement effacées après 15 jours, atteste qu'il y a bien enregistrement et conservation des données ce qui constitue donc un traitement de données au sens de la L.V.P. Le fait pour « Nice people » d'inviter les membres « à lui communiquer les adresses courriels de tiers et, une fois en sa possession, (d')utilise(r) ces adresses pour envoyer le mail », constitue pour la cour des « opérations correspondant assurément à un traitement de données à caractère personnel ».

La profession de détective privé est organisée par une législation particulière, la loi du 19 juillet 1991, et est soumise à la loi générale de protection de la vie privée. La cour d'appel de Mons a rendu le 2 mars 2010 un jugement concernant la profession de détective privé[379]. Un agent immobilier V. accusait un concurrent F. de concurrence déloyale car celui-ci proposait ses services en tant qu'agent immobilier en utilisant le numéro d'agréation de sa compagne. Pour récolter les preuves de ce qu'il avançait, V. engagea un détective privé qui établit un rapport d'inspection au moyen d'un logiciel de traitement de texte. Ce rapport indiquait qu'il s'était rendu dans l'agence de F. en se faisant passer pour un amateur potentiel d'un immeuble, qu'ils avaient échangé des mails et des coups de téléphone, tout cela dans le but de constater l'exercice de la profession d'agent immobilier de F. sans agréation. Le recours à un détective privé est autorisé en vue de réunir des éléments de preuve à la condition qu'il soit « compatible avec le respect de la vie privée et familiale, et avec les dispositions de la loi du 8 décembre 1992 »[380]. Selon le juge, « le rapport d'un détective privé constitue en effet un traitement de données à caractère personnel au sens de la loi du 8 décembre 1992 lorsque, comme en l'espèce, il contient pareilles ''données'', à savoir toute information se rapportant à une personne physique identifiée ou identifiable, lorsque ces données ont subi un ''traitement automatisé'', à savoir tout traitement dans lequel l(es) technologie(s) de l'information (et de la communication) intervien(nent), tel que le traitement de texte utilisé en informatique »[381].

378 Liège (7e ch.), 19 novembre 2009, *D.A. O.R.*, 2010/96, pp. 451 et s.

379 Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, pp. 80 et s.

380 *Ibidem*, p. 82.

381 « Si un tel raisonnement venait à être généralisé, nul doute qu'il mettrait de sérieux bâtons dans les roues dans l'exercice de la profession de détective privé puisqu'il impliquerait que celui-ci doive décliner son nom réel, sa qualité, l'identité de son commanditaire ainsi que la finalité de ses visites avant même de pouvoir procéder à un quelconque acte impliquant un traitement de données à caractère personnel ». F. Dumortier, « La loi du 8 décembre 1992, un obstacle au métier de détective privé, *R.D.T.I.*, n° 41/2010, p. 86.

Enfin, dans l'affaire déjà mentionnée impliquant le Front National, la cour d'appel de Bruxelles a confirmé que la collecte, l'enregistrement dans une liste de diffusion et l'utilisation dans un mailing d'une adresse mail sont bien des traitements au sens de la L.V.P.[382]

103. Responsable du traitement des données à caractère personnel. Le traitement de données est réalisé par le responsable de traitement, qui est défini dans la L.V.P. comme étant « 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 »[383].

Une fois de plus, ce sont les décisions abordant les questions de la profession de détective privé et du marketing viral qui fournissent des précisions quant à l'application de cette notion.

Le rapport d'un détective privé étant un traitement de données à caractère personnel, l'individu qui l'a rédigé doit dès lors être considéré comme le responsable du traitement d'après la cour d'appel de Mons (voy. *supra*). Or et conformément à la L.V.P., certaines obligations lui incombent, notamment « celle d'informer – préalablement à la mise en œuvre du traitement et au plus tard au moment où les données sont obtenues – la personne concernée » de l'existence du traitement et de ses finalités, entre autres. Cela signifie que « le détective devra donc indiquer pour qui il intervient et à quoi vont servir les renseignements demandés ; lorsque les données font l'objet d'une collecte indirecte auprès d'un tiers, cette information doit être communiquée dès l'enregistrement des données »[384]. La cour a rejeté les éléments de preuve issus du rapport du détective privé, l'obligation d'information visée à l'article 9 de la L.V.P. n'ayant pas été respectée en l'espèce.

Dans l'affaire du 19 novembre 2009 relative à la problématique du marketing viral[385], le site de rencontres Nice people remettait en cause sa qualité de responsable de traitement pour l'envoi de mails publicitaires. En effet, il « attribue la qualité de responsable du traitement non à lui-même, mais à la personne qui décide d'inviter son ami ou son amie ». Dès lors, il considère que ce traitement entre dans le champ de l'exclusion pour activités personnelles et domestiques de l'article 3, § 2 de la L.V.P. Nice people « se définit comme simple intermédiaire technique, sous-traitant de celui qui envoie le mail ; l'émetteur étant selon lui le responsable du traitement ». La cour d'appel de Liège n'a pas suivi ce raisonnement. Pour elle, selon la L.V.P., le responsable du traitement est la personne qui détermine les finalités et les moyens du traitement. En l'occurrence, Nice people n'est pas qu'un simple intermédiaire technique car c'est bien lui qui fixe la finalité, celle-ci étant l'inscription sur son site de la personne contactée par courriel.

104. Légitimité des traitements. En vertu de l'article 4, § 2, de la L.V.P., les données à caractère personnel doivent être traitées pour des finalités déterminées, explicites et légitimes. À plusieurs reprises, des jugements ont illustré la question de la légitimité des traitements de données à caractère personnel.

382 La C.V.P. a émis une recommandation sur le marketing direct dans laquelle elle traite spécifiquement des traitements effectués dans ce cadre (recommandation n° 04/2009 du 14 octobre 2009 sur le marketing direct et la protection des données à caractère personnel).

383 Article 3 de la L.V.P.

384 Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, p. 83.

385 Liège (7e ch.), 19 novembre 2009, *D.A. O.R.*, 2010/96, pp. 451 et s.

Même si ce n'était pas l'objet principal de l'affaire « Test-Achats », il est intéressant de relever que la cour a procédé à une balance des intérêts entre, d'une part, la protection des données à caractère personnel et d'autre part, le préjudice qui pourrait être subi par l'entreprise sujette aux critiques sur le forum de Test-Achats. La cour a considéré que la vie privée l'emportait sur un éventuel préjudice et a dès lors ordonné la restitution par Test-Achats des données d'identification en cause. Cette décision de la cour d'appel de Liège a été confirmée par la Cour de cassation dans un arrêt du 16 juin 2011[386] qui a décidé que « cette disposition ne confère pas à une personne qui soutient être victime de propos calomnieux ou diffamatoires publiés sur le site d'un prestataire de services le droit subjectif d'obtenir d'une juridiction de l'ordre judiciaire qu'elle ordonne à ce prestataire de lui communiquer toutes les informations dont elle dispose sur les prétendus auteurs d'infractions aux fins de poursuivre une action civile en réparation »[387]. Il faut souligner le raisonnement de la Cour de cassation sur ce point car en aucun cas le second alinéa de l'article 21, § 2, de la LSSI n'offre à toute personne qui s'estimerait victime de propos calomnieux ou diffamatoires un droit subjectif d'obtenir des informations auprès des autorités compétentes qui permettraient de poursuivre civilement les auteurs de ces propos[388].

Une autre affaire concernait une personne qui avait accès au registre national (ci-après « RN ») dans le cadre de son travail et qui a été licenciée par son employeur pour motif grave car elle a fait usage de données issues de ce registre pour harceler deux individus qu'elle considérait responsables de la mort de l'un de ses proches. La cour du travail de Liège a estimé que « (l)a consultation du registre national à des fins privées n'est pas autorisée. Si les données consultées sont des données confidentielles, qu'elles sont divulguées et que la consultation n'est pas occasionnelle, la faute commise est d'autant plus grave »[389]. Or, « les personnes qui ont accès au registre national sont tenues au secret professionnel conformément à l'article 11 de la loi du 8 août 1983 organisant un registre national des personnes physiques (…) ». Et la Cour ajoute que « (s)i la consultation est ainsi à raison réglementée par la loi, il n'empêche que l'obtention de certains renseignements est moins grave que l'obtention d'autres. Ainsi en va-t-il de l'adresse lorsque celle-ci peut être plus ou moins aisément obtenue via d'autres banques de données telles que celle d'un opérateur téléphonique »[390].

Dans le cadre de l'arrêt de la cour d'appel de Bruxelles du 17 mars 2010, dont nous avons déjà traité à plusieurs reprises précédemment, il a été décidé que le traitement ne peut être effectué que dans l'un des cas prévus par l'article 5, en l'occurrence le consentement indubitable qui doit être fourni par la personne concernée, condition qui n'est pas remplie dans l'affaire. La cour soulève qu'« en cas de contestation, il appartient au responsable du traitement des données d'établir qu'une personne qui conteste a, sans réserve, marqué son assentiment à figurer dans le fichier »[391].

386 Cass., 16 juin 2011, *R.D.T.I.*, n° 47/2012, pp. 69 et s., note H. Jacquemin.

387 Pour plus de détails sur cette affaire, voy. le commentaire d'H. Jacquemin, « Qui peut obtenir les informations permettant de rechercher et de poursuivre les auteurs d'infractions commises sur les réseaux ? », *R.D.T.I.*, n° 47/2012, pp. 74 et s.

388 *Ibidem*, p. 77.

389 C.T. Liège, 10 novembre 2009, R.G. n° 8631/08, p. 8.

390 *Ibidem*, p. 9.

391 Bruxelles (11e ch. corr.), 17 mars 2010, *R.D.T.I.*, n° 42/2011, p. 53.

Dans l'affaire « Nice people » s'était également posée la question de savoir si un site internet qui procède à du marketing viral pouvait invoquer le bénéfice de l'article 5, f), de la L.V.P. « Le recours à cette disposition impose une balance des intérêts en présence, à savoir ceux du responsable du traitement et ceux de la personne concernée »[392]. Il est indéniable que l'objectif de Nice people est de développer son site de rencontres et de lui procurer d'importants revenus publicitaires. Dans son arrêt du 19 novembre 2009, la cour d'appel de Liège va estimer que « s'il peut être admis que les finalités de promotion et de prospection commerciale sont légitimes, elles sont néanmoins primées par les droits fondamentaux de la personne concernée, dont le droit à la protection de sa vie privée »[393].

105. Proportionnalité. Dans un arrêt du 10 novembre 2011, la Cour constitutionnelle a eu l'occasion de rappeler que « toute ingérence des autorités dans le droit au respect de la vie privée [doit être] prévue par une disposition législative suffisamment précise »[394] outre qu'elle doit répondre « à un besoin social impérieux » et qu'elle doit être « proportionnée au but légitime qui est poursuivi »[395].

Cet arrêt a été rendu dans le cadre d'une requête en annulation déposée contre la loi du 21 janvier 2010 modifiant la loi du 25 juin 1992 sur le contrat d'assurance terrestre en ce qui concerne les assurances du solde restant dû pour les personnes présentant un risque de santé accru. En vertu de cette loi, la Commission des assurances devait établir un code de bonne conduite à défaut de quoi le Roi était habilité à régler la question des questionnaires médicaux dans le cadre des assurances du solde restant dû pour les personnes présentant un risque de santé accru. La Cour a estimé que « le législateur a pu estimer que l'utilisation de ces questionnaires devait être réglementée afin d'éviter que, dans le cadre de la conclusion d'un contrat d'assurance, des questions qui ne sont pas pertinentes ou qui sont excessives soient posées et qu'il soit ainsi porté atteinte de manière disproportionnée au droit au respect de la vie privée des intéressés. Il a également pu estimer que le fait que les assureurs exigent un examen médical complémentaire et demandent les résultats de celui-ci, en plus de l'utilisation d'un questionnaire médical, pouvait constituer une restriction disproportionnée du droit au respect de la vie privée de l'intéressé dans les cas où le montant assuré demeure limité »[396]. La Cour a clairement rappelé que la proportionnalité devait être analysée au niveau des données afin d'éviter que des données non nécessaires à la finalité ne soient traitées.

Dans le cadre d'une question préjudicielle posée par la Cour de cassation sur la violation ou non de l'article 22 de la Constitution par l'ancien article 323 du Code civil, la Cour constitutionnelle a eu l'occasion de s'interroger sur la question de proportionnalité d'une loi par rapport au droit de protection de la vie privée. Elle a estimé que le fait que « la recherche de paternité sur la base de la disposition en cause ne pouvait avoir lieu que lorsque la paternité n'avait pas été corroborée

392 Liège (7e ch.), 19 novembre 2009, *D.A. O.R.*, 2010/96, p. 455.

393 *Idem*.

394 Cour const., 10 novembre 2011, 166/2011, www.const-court.be, B.35.3. Il faut relever que cette exigence permet au justiciable de pouvoir contrôler l'ingérence et sa légalité. Voy. également Cour eur. D.H., arrêt *Rotaru c. Roumanie* du 4 mai 2000, *Rev. trim. dr. h.*, 2001, pp. 137-183, obs. O. De Schutter.

395 *Ibidem,* 392 ; nous soulignons.

396 Cour const., 10 novembre 2011, 166/2011, www.const-court.be, B.16.7.

par la possession d'état »[397] « constitue une atteinte disproportionnée au droit au respect de la vie privée des enfants [et] n'est donc pas compatible avec l'article 22 de la Constitution »[398].

Par contre, un arrêt du 18 mars 2010[399] surprend quelque peu. En effet, la Cour constitutionnelle s'est prononcée sur le caractère raisonnable de l'utilisation du numéro de registre national comme clé d'identification dans le cadre de la mise en place de la plateforme eHealth par l'État belge en estimant que « compte tenu des garanties prévues par la loi du 21 août 2008 quant à la confidentialité des données à caractère personnel relatives à la santé au cours de leur traitement par la plateforme eHealth, le choix de recourir au numéro du registre national comme clé d'identification est raisonnablement justifié »[400]. La Cour a donc estimé que la confidentialité permettait d'être une clé d'analyse du caractère nécessaire ou raisonnable telle que demandée par l'article 22 de la Constitution et, avant lui, par l'article 8 de la Convention européenne des droits de l'homme. Cette analyse est quelque peu étrange, dès lors que le caractère nécessaire doit être analysé comme un choix de la voie la moins intrusive dans la vie privée de l'individu. Or, il ne peut être considéré que la confidentialité réponde à cette question ou, même, la résolve. Cet arrêt donne le sentiment de faire passer la sécurité/confidentialité comme une garantie de proportionnalité alors qu'il n'en est rien puisque la sécurité est une obligation à charge du responsable de traitement tandis que le concept de nécessité se situe au niveau du traitement lui-même et des données. Sécurité ne peut pas signifier nécessité.

106. Droits de la personne concernée. C'est en vertu de l'article 9 de la L.V.P. que le responsable du traitement doit informer la personne concernée notamment de l'existence d'un droit d'accès à ses données, et ce, qu'il les ait obtenues directement ou indirectement.

Le 17 mars 2010, la cour d'appel d'Anvers a rendu un arrêt dans une affaire concernant une personne résidant dans une maison de repos qui souhaitait avoir accès et obtenir une copie de son dossier de soins. La cour ayant estimé que la loi relative aux droits du patient[401], et plus particulièrement son article 9, ne s'appliquait pas, c'est vers les dispositions de la loi vie privée qu'elle s'est tournée. Cette dernière prévoit en son article 10, § 2, que toute personne a le droit, soit directement, soit avec l'aide d'un praticien professionnel en soins de santé, de prendre connaissance des données à caractère personnel traitées en ce qui concerne sa santé. Cependant, la cour va considérer que ce droit d'accès n'implique pas l'imposition d'un droit à une copie des données médicales du dossier de soin[402].

Dans le cas d'une demande de consultation par un patient de son dossier médical constitué et détenu par l'assureur, c'est sur la base des deux lois mentionnées ci-dessus, que le patient pourra exiger cette consultation. La cour a décidé qu'« en vertu de l'article 9 de la loi du 22 août 2002 relative aux droits du patient, le fonds d'assurance est tenu de délivrer à la personne assurée non seulement le dossier médical constitué par l'assureur au sujet du dommage subi par l'assuré, mais

397 Cour const., 7 juillet 2011, 122/2011, B.2.

398 Cour const., 7 juillet 2011, 122/2011, B.8. Voy. également Cour const., 3 février 2011, 20/2011, www.const-court.be au sujet de l'article 318, § 1er, du Code civil.

399 Cour const., 10 novembre 2011, 166/2011, www.const-court.be.

400 Cour const., 18 mars 2010, 29/2010, www.const-court.be.

401 Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 26 septembre 2002, p. 43698.

402 Anvers (8e ch.), 17 mars 2010, *Revue de droit de la santé*, 2011/2012, p. 20.

aussi, en vertu de la loi du 8 décembre 1992 relative à la vie privée, toute information recueillie par cet assureur à son sujet ».

107. Preuve. Une preuve recueillie illicitement peut être acceptée par un juge à la condition que son obtention ne soit pas entachée d'un vice qui serait préjudiciable à sa crédibilité ou porterait atteinte au droit à un procès équitable[403]. Cette règle peut notamment être appliquée dans des cas d'enregistrement audio, de vidéosurveillance, etc. pour apporter la preuve d'un fait allégué.

Le 17 mars 2010, la Cour de cassation a été saisie d'une affaire dans laquelle la preuve d'une scène de coups était rapportée à l'aide d'une caméra de vidéosurveillance installée dans la rue[404]. Le demandeur en cassation reprochait au juge d'appel d'avoir refusé d'écarter du dossier cet enregistrement qui violait selon lui l'article 8 de la Convention européenne des droits de l'homme ainsi que les articles 4, 5, 8 et 9 de la L.V.P. La Cour va estimer que les juges d'appel ont légalement décidé que l'enregistrement ne portait pas atteinte à la vie privée du demandeur – et donc n'était pas prohibé par l'article 8 de la Convention européenne des droits de l'homme – en considérant que « de la seule circonstance qu'une caméra de surveillance, installée visiblement sur la voie publique, permet de réunir des éléments de preuve des infractions qui s'y commettent, il ne saurait se déduire une ingérence dans l'exercice du droit au respect à la vie privée ». Remarquons que les juges d'appel, suivis par la Cour de cassation, n'ont pris en compte que l'article 8 de la Convention européenne des droits de l'homme et non la L.V.P., pourtant soulevée par les demandeurs, pour parvenir à une telle conclusion. D'autre part, les juges d'appel, également suivis par la Cour de cassation sur ce point, ont jugé que « concernant le comportement du demandeur sur la voie publique, les scènes filmées et enregistrées ne mettent pas en cause son intimité ». Les juges d'appel n'ont à nouveau pas fait référence à la L.V.P. telle qu'elle avait été avancée par les demandeurs.

Les conversations téléphoniques, *a priori* protégées par le droit au respect de la vie privée sur la base de l'article 8 de la Convention européenne des droits de l'homme, ne peuvent cependant être systématiquement exclues en tant que preuve sur cette base. Ce sera donc à la juridiction saisie de procéder à un test de proportionnalité entre l'établissement de la preuve et le droit au respect de la vie privée, en examinant si la preuve n'aurait pu être apportée d'une manière moins attentatoire aux droits de la personne concernée[405]. Le tribunal de première instance de Gand a, quant à lui, apporté deux éléments d'appréciation supplémentaires, premièrement en évaluant le contenu d'une conversation et, deuxièmement en jugeant du contexte dans lequel a eu lieu ladite conversation téléphonique[406]. Dans cette affaire, le juge devait notamment évaluer la recevabilité d'une conversation téléphonique enregistrée par un journaliste à l'insu d'une personne issue du monde du sport. Par cette conversation, le journaliste visait à obtenir la preuve de faits allégués dans un livre traitant du dopage et qui n'était pas encore paru. Concernant le premier élément d'appréciation, il a été considéré que la conversation ne contenait pas de confidence particulière par rapport à ce qui était écrit dans le livre. Quant au second élément, le tribunal a jugé que la conversation n'avait pas eu lieu dans un climat de confiance mutuelle entre les parties

403 Cass., 10 mars 2008, www.cass.be.
404 Cass., 17 mars 2010, *R.W.*, 2011-12, n° 30, 24 mars 2012, pp. 1332 et s.
405 Gand (14e ch.), 16 février 2010, *T.G.R.*, 2010, p. 258.
406 Civ. Gand, 26 mars 2010, *NjW*, 2010, p. 546.

et que dès lors il n'y avait pas eu de violation sur la base de l'article 8 de la Convention européenne des droits de l'homme.

Dans une procédure de plainte pour harcèlement sur le lieu de travail, la cour du travail de Liège a accepté comme preuve un enregistrement effectué par la plaignante lors d'une réunion professionnelle. La partie adverse avait soulevé que ledit enregistrement violait son droit à la vie privée selon les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme, mais la cour a observé que « les propos tenus ne revêtent aucunement le caractère privé que (la partie adverse) entend leur conférer (…), puisqu'il ne peut être perdu de vue que cette conversation a eu lieu au cours d'une réunion professionnelle du service et ce, peu importe que l'intimée y ait été ou non conviée »[407].

La Cour de cassation va estimer que ne viole pas la vie privée le fait pour un détenteur régulier de lettres ou de courriels – la Cour ne nous dit pas ce qu'elle entend par « détenteur régulier » – de les utiliser « comme moyens de preuve dans un procès qui tend à faire prononcer des mesures provisoires au cours d'une procédure en divorce »[408]. Il est dommage que la Cour de cassation n'ait pas profité de cet arrêt pour donner une lecture fonctionnelle de la loi du 13 juin 2005 relative aux communications électroniques qu'elle n'aborde même pas.

Le 7 novembre 2011, la cour d'appel de Bruxelles a considéré que la L.V.P. ne faisait pas obstacle à la production de courriels dans une procédure en divorce tant qu'un moyen illicite n'avait pas été utilisé pour entrer en leur possession. De plus, aucune infraction à l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques n'est établie car il n'a pas été prouvé que la partie « n'a pas elle-même rendu possible l'accès aux pièces produites par (l'autre partie) ». Dans de telles affaires où la notion de faute commise par l'un des conjoints doit être appréciée, il doit être admis « que des éléments de l'intimité de la vie des parties soient révélés et invoqués par celles-ci »[409].

Enfin, encore dans le cadre d'une procédure en divorce, la cour d'appel de Gand a jugé que la production en justice d'extraits de conversations en ligne obtenus par intrusion du mari dans l'ordinateur portable de l'enfant mineur du couple, et cela sans l'autorisation de ce dernier âgé de 17 ans, n'est pas licite[410]. La cour précisant que l'enfant mineur est au seuil de sa majorité, nous pouvons en déduire que cela a influencé le raisonnement de la cour qui considère que « l'exercice de l'autorité parentale est limité par les droits de la personnalité de l'enfant qui sont d'autant plus étendus que l'enfant approche de sa majorité ».

Un arrêt de la Cour constitutionnelle du 22 décembre 2010 a été rendu sur questions préjudicielles posées par le tribunal correctionnel de Gand. Le tribunal se posait la question d'une éventuelle violation du droit au respect de la vie privée tel que consacré par l'article 22 de la Constitution par l'article 34, § 1er, alinéa 2, de la loi du 5 août 1992 sur la fonction de police « dans l'interprétation selon laquelle la méconnaissance de celui-ci, lors d'un contrôle d'identité illégal, ne conduit pas nécessairement à la nullité de la preuve obtenue ». Par ailleurs, le tribunal correctionnel se posait

407 C.T. Liège, 10 septembre 2010, p. 12.
408 Cass., 1er avril 2011, www.cass.be, p. 3.
409 Civ. Bruxelles (3e ch.), 7 novembre 2011, *Rev. trim. dr. fam.*, 1/2012, p. 167.
410 Gand, 23 avril 2009, *R.A.B.G.*, 2010/2012, p. 807.

la question d'une éventuelle inégalité non autorisée entre cet article 34, § 1er, alinéa 2, dans l'interprétation mentionnée ci-dessus, dès lors que la loi ne prévoyait aucune sanction de nullité, tel que c'était le cas dans d'autres textes législatifs, alors qu'il s'agit toujours de la garantie de droits fondamentaux, ce qu'est le droit au respect de la vie privée. Après avoir énuméré plusieurs arrêts de la Cour européenne des droits de l'homme de Strasbourg relatifs à la question des éléments de preuve obtenus en méconnaissance de l'article 8 de la Convention européenne des droits de l'homme, la Cour considère qu'ils faisaient apparaître « d'une part, que la Cour européenne des droits de l'homme a jugé que les articles 6 et 8 de la Convention européenne ne comportent pas de règles concernant l'admissibilité d'une preuve dans une affaire et, d'autre part, que l'utilisation d'une preuve obtenue en méconnaissance de l'article 8 de cette Convention ne conduit pas nécessairement à une violation du droit à un procès équitable garanti par l'article 6.1. de la Convention européenne »[411]. Elle poursuit en considérant qu'« il s'ensuit que la circonstance qu'une preuve obtenue en méconnaissance d'une disposition légale visant à garantir le droit au respect de la vie privée n'est pas automatiquement nulle, ne viole pas en soi le droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme » et que « l'article 22 de la Constitution, qui garantit également le droit au respect de la vie privée, ne comporte pas plus que l'article 8 de la Convention européenne des droits de l'homme une règle explicite relative à l'admissibilité de la preuve obtenue en méconnaissance du droit garanti pour celui-ci »[412].

La question préjudicielle a donc reçu une réponse négative dès lors que l'article 22 de la Constitution « n'exige pas en soi qu'une preuve obtenue en méconnaissance du droit qu'il garantit doit être considérée comme nulle en toute circonstance ».

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

Elise Degrave[413]

108. L'e-gouvernement. L'e-gouvernement, appelé également « administration électronique », peut être défini comme l'utilisation des technologies de l'information et de la communication dans le secteur public, associée aux changements qu'elle engendre au niveau de la structure et du fonctionnement des administrations[414].

Ce phénomène récent met en exergue la nécessité de trouver un équilibre entre l'efficacité administrative, d'une part, la protection de la vie privée des citoyens, d'autre part.

Cette recherche d'équilibre mérite d'autant plus d'attention que les institutions publiques détiennent une multitude d'informations sur les citoyens, que ces derniers ont été contraints de leur donner. Certes, les outils informatiques nouveaux facilitent et perfectionnent l'action administrative en permettant désormais aux administrations de s'échanger ces informations, de dresser des profils de fraudeurs, voire même de vendre ces informations à des sociétés de marketing. Mais, dans le même temps, ces progrès confèrent aux pouvoirs publics toujours plus

411 Cour const., 22 décembre 2011, 158/2010, www.const-court.be, B.6.3.

412 *Ibidem*, 409, B.6.4.

413 Assistante à la Faculté de droit de l'Université de Namur et chercheuse au CRIDS (www.crids.eu).

414 E. Degrave, *L'administration électronique et la protection de la vie privée. Légalité, transparence et contrôle.* Thèse en cours de rédaction.

de puissance face aux citoyens qui risquent dès lors de perdre la maîtrise de leurs informations personnelles.

Dans ce contexte, les avis de la Commission de la protection de la vie privée (ci-après « la Commission ») guident les réflexions relatives à l'organisation d'un e-gouvernement respectueux des droits et libertés des citoyens, en insistant sur les garanties qui doivent accompagner la mise en place des nouveaux outils et des nouvelles opérations à disposition de l'administration[415].

a. Les nouveaux outils

109. Les intégrateurs et la source authentique de données. L'administration électronique fait émerger des concepts nouveaux correspondant à des réalités techniques parfois complexes. Les avis de la Commission permettent d'en saisir pleinement le sens.

1° Les intégrateurs

110. La notion et l'encadrement. Deux types d'intégrateurs doivent être distingués, dont la légalité exige le respect de certaines garanties.

111. Les intégrateurs de service et de données. Dans une importante recommandation d'initiative concernant les intégrateurs dans le secteur public[416], la Commission se penche sur la manière d'organiser la mise à disposition, au bénéfice d'une administration, de données provenant de plusieurs sources différentes dans le respect du régime de la protection des données à caractère personnel.

À cette occasion, elle livre sa définition de deux outils nouveaux, à savoir, l'intégrateur de services et l'intégrateur de données.

L'intégrateur de services est défini comme « l'harmonisation de services électroniques partiels en un ensemble cohérent de services électroniques en vue de le proposer à des tiers ». Le modèle de la Banque-carrefour en est un exemple[417].

L'intégrateur de données est défini comme « l'agrégation de données à caractère personnel provenant de plusieurs sources authentiques et leur enregistrement dans une banque de données intégrée distincte, en vue de leur communication à des tiers »[418]. Le modèle d'intégrateur de services flamand (ISF) en est un exemple.

i. L'encadrement de l'intégrateur

112. La finalité du traitement. La Commission rappelle que l'utilisation d'un intégrateur n'est permise que lorsqu'elle poursuit un objectif qui s'inscrit dans une ou plusieurs hypothèses visées

415 À défaut de pouvoir prétendre à l'exhaustivité, la présente analyse de jurisprudence se concentre sur les avis majeurs de la Commission qui précisent ou modifient les enseignements antérieurs à 2009 concernant les outils et les opérations d'e-gouvernement destinés au fonctionnement du *back office*.

416 Recommandation n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public.

417 *Ibidem,* n° 2.

418 *Idem*.

à l'article 5, alinéa 1er, de la L.V.P.[419] tel que la nécessité au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Concernant en particulier l'intégrateur de services, la Commission précise que « vu son impact, l'intégration de services doit être considérée comme une finalité distincte et pas simplement la dérivée d'une autre finalité ou inhérente à celle-ci » car « la finalité ''intégration de services'' est (…) un critère à l'aide duquel tous les aspects de ce processus d'intégration doivent être évalués, notamment en ce qui concerne leur lien avec la finalité »[420].

113. La proportionnalité du traitement. D'emblée, la Commission encourage le recours à un intégrateur de services, au nom de l'exigence de proportionnalité du traitement. En effet, l'intégrateur de service « constitue dans la plupart des cas une option moins menaçante pour la vie privée [que] l'intégration de données à caractère personnel »[421].

Elle justifie cette affirmation en soutenant notamment que « dans le cas d'une intégration de services, les données ne sont agrégées que temporairement, à savoir au moment de l'offre du service intégré (…). Un tel service n'exige pas l'agrégation permanente de données, ni leur enregistrement intégré à plus long terme. Généralement, les données sont directement obtenues auprès de différentes banques de données fiables, sous la responsabilité d'entité déterminée, ce qu'on appelle des sources authentiques »[422].

Ce faisant, « on évite la circulation inutile de copies de fichiers de données dans lesquels sont enregistrées des données à caractère personnel qui ne sont pas régulièrement mises à jour et qui, par conséquent, contiennent des informations dépassées – donc des erreurs – ce qui doit être évité à la lumière de l'article 4, 1°, de la L.V.P. Cela réduit en outre le risque d'accès illégitime aux données à caractère personnel étant donné que celles-ci ne sont pas reprises inutilement en plusieurs copies à plusieurs endroits »[423].

114. Le champ d'action de l'intégrateur de services et le répertoire de références. La mise en œuvre de l'exigence de proportionnalité du traitement aboutit à préférer l'intégrateur de services à l'intégrateur de données mais également à limiter le champ d'action de l'intégrateur de services. Celui-ci « doit être clairement délimité et être suffisamment homogène afin qu'un utilisateur potentiel dispose d'un interlocuteur clair pour un domaine spécifique et qu'une application univoque de normes et de mesures de sécurité et de protection de la vie privée soit garantie »[424].

En outre, l'utilisation d'un répertoire de références peut s'avérer utile pour gérer le champ d'action de l'intégrateur de services. « Un tel répertoire peut constituer la base de l'organisation de l'échange électronique de données et peut se composer de tableaux reliés entre eux » à savoir, « un tableau des (…) informations disponibles qui mentionne (…) quelles informations sont

419 *Ibidem,* n° 16.
420 *Ibidem,* n° 18.
421 *Ibidem,* n° 6.
422 *Ibidem,* n° 7.
423 *Ibidem,* n° 8.
424 *Ibidem,* n° 22. Pour un cas d'application de cette exigence, voy. l'avis n° 28/2009 du 14 octobre 2009 relatif à un projet d'arrêté royal modifiant l'arrêté royal du 16 janvier 2002 relatif à l'extension du réseau de la sécurité sociale à certains services publics et institutions publiques des Communautés et des régions, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

disponibles auprès d'un acteur» (tableau «quoi-où»), «un tableau d'utilisateurs (…) ayant reçu un accès (…) [ainsi que] les profils d'accès» (tableau «qui reçoit quoi») et, enfin, «un répertoire de personnes qui indique quelles personnes, en quelle qualité, possèdent des dossiers auprès de quels acteurs concernant quelles périodes» (tableau «qui-où-comment-quand»)[425].

ii. La transparence des traitements de données effectués par l'intégrateur

115. Le citoyen n'est pas un objet passif. La Commission reconnaît que «pour le citoyen, une intégration de services ne sera pas toujours transparente»[426]. Or, il «ne peut toutefois être relégué au rang d'objet passif de cette évolution»[427]. C'est pourquoi, «il faut à tout prix éviter que le citoyen soit découragé d'exercer ses droits parce qu'il lui est impossible d'identifier le(s) bon(s) interlocuteur(s)»[428].

116. La publication d'informations. Partant de ce constat, la Commission soutient qu'il importe de publier «des informations claires concernant toutes les facettes [du fonctionnement de l'intégrateur de service]» tel que son objectif[429], d'assurer la publication des autorisations d'échange[430], et de communiquer au citoyen «sur quelles données [l'utilisateur] base une décision ou une action afin que le citoyen puisse contrôler si l'on a travaillé avec les données correctes»[431].

Il s'impose également de définir quelle instance participant à l'intégrateur tient à jour quels *loggings*, ainsi que «puisse avoir lieu, lors d'un examen effectué à l'initiative d'un organe de contrôle ou à l'occasion d'une plainte, un traçage complet (quoi, quoi, où, quand, pourquoi) de la personne physique qui a utilisé quel service ou quelle transaction concernant quel citoyen ou quelle entreprise, quand, via quel canal et pour quelles finalités»[432].

2° La source authentique de données

117. La notion et l'encadrement. La source authentique de données est une notion récente que la Commission n'a pas manqué d'éclairer, en insistant sur les garanties que le législateur doit organiser à ce sujet.

i. La notion de source authentique de données

118. Plusieurs garanties. Selon la Commission, pour mériter la qualité de source authentique, une base de données doit respecter «des garanties dans quatre domaines, à savoir concernant la qualité des données, l'utilité de la source de données, son caractère opérationnel et la sécurité»[433]. S'agissant en particulier de la qualité des données, elle mentionne des critères plus précis

425 *Ibidem,* n° 25.
426 *Ibidem,* n° 21.
427 *Ibidem,* n° 35.
428 *Ibidem,* n° 21.
429 *Ibidem,* n° 33.
430 *Ibidem,* n° 35.
431 *Ibidem,* n° 35.
432 Avis n° 11/2009 du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 208 relatif à l'échange électronique de données administratives, n° 39.
433 *Ibidem,* n° 8.

« à l'aide desquels le contrôle concret devra être effectué »[434] que sont « l'exhaustivité, l'exactitude, l'actualité, la manière dont la qualité est garantie, la traçabilité des modifications apportées aux données et la conservation de l'historique de l'accès aux données »[435].

119. Un outil recommandé par la Commission. La Commission encourage la mise en place de sources authentiques de données au sein de l'administration, comme elle l'a rappelé à l'occasion de l'organisation de l'échange électronique de données administratives en Flandre[436].

En effet, « dans le cadre de processus d'e-gouvernement, des données fautives ont (…) un effet domino qui n'est profitable ni aux autorités souhaitant recourir à ces données, ni au citoyen qui espère un service de grande qualité »[437]. Puisque la source authentique contient des données fiables à valeur unique, elle répond au souci majeur de l'administration électronique d'assurer la qualité des données échangées.

ii. L'encadrement de la source authentique de données

120. Les éléments essentiels de l'outil. Une source authentique de données n'est pas un outil anodin, si bien qu'une administration ne peut décider seule de mettre en place un tel outil. Ce rôle revient au pouvoir législatif. En effet, en vertu « de la lecture conjointe de l'exigence d'une législation transparente visée à l'article 8 de la C.E.D.H., de l'interprétation de l'article 22 de la Constitution par la Cour constitutionnelle et des principes de légalité et de finalité (article 5 c)[438] et/ 5 e) de la L.V.P.[439]) »[440], il importe de permettre aux personnes concernées « de savoir à l'avance qui peut recevoir quelles données pour quelle finalité »[441].

Dès lors, la loi doit mentionner explicitement les éléments essentiels de la source authentique de données que sont la finalité poursuivie, les données enregistrées, les utilisateurs concernés et le responsable du traitement. En outre, des mesures de transparence et un contrôle des accès doivent être organisés.

121. La finalité. La finalité de la source authentique de données doit être *déterminée et légitime.*

Par exemple, la Commission a considéré que la finalité « prévenir et lutter contre les mariages simulés définis à l'article 146*bis* du Code civil » assignée à une nouvelle source authentique de données répond à cette exigence[442]. Cette finalité permet de « vérifier la proportionnalité des données qui seront traitées dans le cadre de la banque de données (article 4, § 1er, 3°, de la

434 *Ibidem,* n° 9.

435 *Ibidem,* n° 9.

436 Avis n° 11/2009 du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 208 relatif à l'échange électronique de données administratives.

437 *Ibidem,* n° 6.

438 Traitement nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

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

440 Avis n° 06/2009 du 18 mars 2009 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, n° 12.

441 *Ibidem,* n° 12. Dans le même sens, voy. l'avis n° 11/2009 précité, n° 33.

442 Avis n° 10/2010 du 31 mars 2010 relatif à l'avant-projet de loi instituant une banque de données en vue de la lutte contre les mariages simulés, n° 14.

L.V.P.) »[443] et de comprendre que ledit traitement de données « reposera sur l'article 5, premier alinéa, f) de la L.V.P. Le SPF Justice mettra les données collectées à disposition des instances qui doivent empêcher et réprimer les mariages simulés »[444].

La finalité doit également apparaître *explicitement* dans la loi[445]. Ainsi, s'agissant de la source authentique des données relatives aux véhicules, la Commission s'est réjouie du fait que le législateur avait suivi ses recommandations antérieures en insérant, dans le texte de l'avant-projet, « une liste détaillée de finalités pour lesquelles les données de la source authentique peuvent être utilisées »[446].

122. Les données. Les données enregistrées dans la source authentique doivent être énoncées dans la loi[447]. La Commission veille attentivement à ce qu'elles soient limitées aux informations réellement nécessaires au regard de la finalité poursuivie par cette base de données[448].

En fonction du type de données enregistrées dans la source authentique, celle-ci peut avoir un caractère positif ou négatif. La Commission le rappelle dans un avis relatif à la constitution d'une base de données en vue de lutter contre les mariages simulés[449].

La base de données a un *caractère positif* « lorsque les informations qui y sont reprises sont objectives et n'étiquettent pas les personnes enregistrées comme des suspects d'un délit ou ne les associent pas à un fait ayant une connotation négative. Du point de vue (…) du principe de proportionnalité (article 4, § 1er, 2° [de la L.V.P.]), l'inconvénient d'une telle banque de données réside dans le fait qu'elle reprend un plus grand nombre de personnes que celui qui peut se justifier sur la base de la finalité »[450]. La Centrale des crédits aux particuliers est, par exemple, une base de données positive.

La base de données a un *caractère négatif* « lorsque, compte tenu de la finalité, seules sont enregistrées les personnes concernant lesquelles certains constats ont été établis ou du moins pour lesquelles il existe des indications. Une banque de données qui est conçue de la sorte est moins problématique du point de vue du principe de proportionnalité mais le fait d'y être enregistré est un signe (suspect à l'égard d'un fait, lien avec quelque chose de négatif) »[451]. Tel est le cas des listes noires telle était celle reprenant les locataires défaillant mise en place par le Syndicat National des Propriétaires[452].

443 *Ibidem,* n° 15.

444 *Ibidem,* n° 16.

445 Au sujet de cette exigence dans la jurisprudence de la Commission de la protection de la vie privée antérieure à 2009, voy. E. Degrave, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée, *C.D.P.K.*, 2009, pp. 46-71.

446 Avis n° 06/2009 précité, n° 4.

447 *Ibidem,* n° 12.

448 Avis n° 14/2010 du 31 mars 2010 relatif à un avant-projet de loi portant création de la Banque-carrefour des permis de conduire, n° 40.

449 Avis n° 10/2010, précité.

450 *Ibidem,* n° 9.

451 *Ibidem,* n° 10.

452 Avis n° 52/2002 du 19 décembre 2002.

La Commission réclame du législateur qu'il examine consciencieusement les avantages et les inconvénients de chaque type de base de données au moment d'instituer une nouvelle source authentique de données[453].

123. Les utilisateurs. « Les utilisateurs existants (…) et les catégories potentielles d'utilisateurs »[454] doivent figurer dans la loi, soit nommément, soit en tant que catégorie[455]. La Commission justifie cette assertion en rappelant qu'il est essentiel pour toutes les personnes concernées par la source authentique de « pouvoir conserver la traçabilité de la communication des données (…) et [de] pouvoir contrôler si les utilisateurs peuvent effectivement utiliser les données avec une base légale suffisante et s'ils respectent le principe de finalité »[456].

Pour la Commission, la désignation des utilisateurs telle que régie par l'avant-projet de loi *portant création de la source authentique des véhicules* est insatisfaisante. En effet, ce texte prévoit deux procédures de désignation distinctes. Peuvent ainsi accéder à la source authentique des véhicules, les utilisateurs ayant obtenu l'autorisation du comité sectoriel compétent, et ceux qui y sont autorisés par un arrêté royal. La Commission désapprouve cette méthode, soulignant qu'« il n'est toujours pas clair de savoir dans quels cas on optera pour quelle procédure » et qu'« il serait souhaitable qu'à l'avenir, les procédures d'accès aux diverses sources authentiques fédérales (registre national, Banque-carrefour des entreprises,…) soient aussi uniformes que possible ». Cela signifie notamment qu'« il peut être utile de stipuler (dans l'exposé des motifs) que le Roi interviendrait si la procédure d'autorisation ne semble pas recommandée parce qu'une intervention réglementaire constitue l'option la plus pratique en raison du nombre de demandeurs (…) ou parce qu'un nombre de mesures réglementaires spécifiques doivent être imposées au(x) demandeur(s) (par exemple, des mesures de sécurité spéciales), ce qui ne relève pas de la compétence du comité sectoriel »[457].

124. Le responsable du traitement. Le pouvoir législatif doit également déterminer l'administration responsable de la source authentique de données. C'est à elle que revient notamment la tâche de veiller à ce que les données utilisées soient correctes et actuelles[458].

À propos de la désignation du SPF Justice en tant que responsable de traitement de la banque de données instituée en vue de lutter contre les mariages simulés, la Commission a estimé « qu'il serait souhaitable que le responsable de traitement soit identifié explicitement dans la disposition légale »[459] et non seulement dans l'exposé des motifs.

125. Les mesures de transparence. Soucieuse de garantir aux citoyens la transparence des traitements de leurs données, la Commission a soulevé la question de savoir « s'il ne serait pas utile de prévoir la possibilité pour le citoyen de contrôler électroniquement ses données dans des sources authentiques. Il pourrait ainsi signaler lui-même des inexactitudes concernant ses

453 *Ibidem,* n° 13.
454 Avis n° 06/2009, précité, n° 12.
455 *Ibidem,* n° 11.
456 *Ibidem,* n° 12.
457 *Ibidem,* n° 19.
458 Avis n° 14/2010, précité, n° 17. Dans cet avis relatif à l'avant-projet de loi portant création de la Banque-carrefour des permis de conduire, la Commission a estimé que la responsabilité de la source authentique revient au SPF Mobilité.
459 Avis n° 10/2010, précité, n° 17.

données ». Et d'ajouter que « ceci requiert évidemment que les mesures de sécurité nécessaires soient prises et plus particulièrement qu'une authentification valable soit exigée afin de garantir que le citoyen ne puisse consulter que ses propres données »[460].

Néanmoins, l'impératif de transparence ne va pas jusqu'à imposer que la personne concernée connaisse le nom du fonctionnaire ayant consulté ses données. Ce serait excessif au regard de l'exigence de proportionnalité des données. Il suffit de faire savoir au citoyen l'instance ayant consulté ses données, de manière à ce qu'il puisse éventuellement s'adresser à cette autorité pour obtenir des explications détaillées. Tel est l'enseignement de la Commission au sujet du registre national[461].

126. Le contrôle de l'accès aux données. La Commission décourage la prolifération d'organes de contrôle des traitements de données.

S'agissant de l'accès à la source authentique constituée pour lutter contre les mariages simulés, elle rappelle l'existence du Comité sectoriel pour l'Autorité fédérale, constitué au sein de la Commission et compétent pour « accorder des autorisations d'accéder à des données à caractère personnel qui relèvent d'une autorité fédérale », en application de l'article 36*bis* de la L.V.P. C'est pourquoi la Commission désapprouve la « création d'un organe de contrôle qui se trouve sous l'autorité des trois ministres de tutelle dont les services contrôlent l'application correcte des diverses dispositions concernant le mariage. Plusieurs questions peuvent (…) se poser quant à l'indépendance d'un organe qui se trouve sous l'autorité ministérielle »[462].

b. Les nouvelles opérations

127. Le contrôle et l'octroi d'avantages. Les technologies de l'information et de la communication permettent à l'administration de contrôler davantage les citoyens, mais également d'optimaliser l'octroi des avantages auxquels ils peuvent prétendre.

1° L'échange d'informations pour contrôler les citoyens

128. Les échanges d'informations entre administrations fiscales. La Commission s'est prononcée sur un avant-projet de loi visant à insérer dans le Code des impôts sur le revenu une disposition organisant l'échange, entre les administrations fiscales, de tous les renseignements permettant d'assurer l'établissement et la perception des impôts[463].

La Commission considère que l'établissement et la perception de l'impôt est une *finalité* légitime[464].

460 Avis n° 11/2009, précité, n° 24.

461 Avis n° 12/2009 du 29 avril 2009 concernant un certain nombre de questions qui se sont posées dans le cadre de la délibération RN n° 19/2008, n° 20. Dans le même sens, voy. recommandation 03/2010 du 9 juin 2010 relative à l'application des « *circles of trust* » (cercles de confiance) et à l'obligation de transparence concernant les consultations des informations du registre national, n° 11.

462 Avis n° 10/2010, précité, n° 36.

463 Avis n° 29/2009 du 28 octobre 2009 relatif à un avant-projet de loi-programme faisant suite à une notification dans le cadre du conclave budgétaire 2010-2011 en matière d'échange de données au sein du SPF Finances (chapitre IV, articles D1 à D8).

464 *Ibidem*, n° 4.

Elle rappelle néanmoins que « tous les agents du SPF Finances ne peuvent (…) sans plus être autorisés à traiter l'ensemble des renseignements en possession de l'administration »[465]. Seuls « les fonctionnaires des administrations fiscales et du SPF Finances régulièrement chargés de l'établissement, de la perception et du recouvrement de l'impôt sont légitimement habilités à traiter des informations et plus spécifiquement des données à caractère personnel, dans le but d'assurer l'établissement, la perception et le recouvrement de l'impôt »[466]. Si tel n'est pas le cas, les agents de l'administration violeraient leur obligation d'agir « dans les limites des lois et règlements qui définissent leurs missions, compétences, pouvoirs et moyens d'action »[467]. En outre, les traitements de données ainsi effectués porteraient atteinte à l'article 4, § 1er, 1°, de la L.V.P., qui prévoit que tout traitement de données doit être loyal et licite ainsi qu'à l'article 5, alinéa 1er, e) de ladite loi, en vertu duquel un fonctionnaire ne peut effectuer que les traitements de données nécessaires à l'exercice de ses missions[468].

Quant aux *données* collectées et traitées, la Commission rappelle qu'elles doivent être adéquates, pertinentes et non excessives, en vertu de l'article 4, § 1er, 3°, de la L.V.P. Elles doivent, en outre, « présenter un rapport de nécessité avec la mission de l'agent qui les requiert ou à qui elles sont transmises ou le compte duquel elles sont collectées »[469].

2° L'échange d'informations pour avantager les citoyens

129. Les échanges d'informations entre CPAS et Office du travail. Un projet d'accord de coopération entre les CPAS et l'Office du travail de la Communauté germanophone a été soumis à la Commission[470]. Cet accord vise à encadrer l'échange des informations relatives aux demandeurs d'emploi qui perçoivent un revenu d'intégration sociale et qui, de ce fait, sont inscrits tant auprès d'un CPAS que de l'Office du travail. Il s'agit de faciliter les démarches administratives de ces personnes, en évitant qu'elles soient radiées de l'Office du travail alors qu'elles sont toujours bénéficiaires d'un revenu d'intégration sociale.

La Commission estime que la *finalité* poursuivie par cet échange de données est légitime au regard de l'article 5, e), de la L.V.P., étant donné qu'elle correspond à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement. En outre, les données échangées répondent à l'exigence de proportionnalité[471].

Néanmoins, ce projet d'accord prévoit que l'échange des informations prendra la forme de listes envoyées par voie postale et/ou par courrier électronique entre les institutions concernées par le dossier d'un même allocataire. La Commission s'oppose à ce système d'échange en rappelant que les CPAS sont des institutions de sécurité sociale. Elles sont dès lors soumises à l'article 14 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation de la Banque-carrefour de la sécurité sociale qui impose à ces autorités de passer par la Banque-carrefour de la sécurité sociale

465 *Ibidem,* n° 7.
466 *Ibidem,* n° 6.
467 *Ibidem,* n° 7.
468 *Idem.*
469 *Ibidem,* n° 8.
470 Avis n° 07/2010 du 17 mars 2010 relatif à un projet d'accord de coopération entre les Centres publics d'action sociale et l'Office du travail de la Communauté germanophone.
471 *Ibidem,* n° 9 à 12.

pour toute communication de leurs données. La communication des données entre les CPAS et l'Office du travail n'échappe pas à cette obligation. En outre, en vertu de cette même loi, les CPAS sont contraints de demander l'autorisation du Comité sectoriel de la sécurité sociale et de la santé avant d'effectuer la communication de ses données. La Commission invite dès lors les CPAS et l'Office du travail « à réparer cet oubli et [à] obtenir une telle autorisation »[472].

130. Le guide des droits. Le guide des droits est un portail internet organisé par un décret flamand, dans le but de faciliter l'accès de chaque citoyen aux droits sociaux fondamentaux garantis aux articles 23 et 24, § 3, de la Constitution.

Le guide des droits présente les avantages auxquels tout citoyen peut prétendre en matière de travail, de revenu, d'enseignement, de culture, etc. Afin d'optimaliser cet outil en offrant, à toute personne qui en fait la demande, un relevé personnalisé des droits pertinents, il est nécessaire d'organiser des échanges électroniques de données entre le guide des droits et différentes sources authentiques de données.

La Commission se montre favorable à de tels traitements de données, moyennant le respect de certaines conditions[473].

Ainsi, il y a lieu d'indiquer dans le décret que le *consentement* des personnes concernées est requis, avant que les données soient réclamées aux différentes autorités concernées[474].

En ce qui concerne la *proportionnalité*, elle approuve le fait que seules les données nécessaires à l'élaboration du profil personnel dressé par le guide des droits seront utilisées. En outre, la Commission exige que ces données ne soient pas conservées après que le citoyen ait obtenu le résultat de la recherche effectuée par le portail[475].

S'agissant du *responsable de traitement* de ce portail, la désignation des « services de l'autorité flamande » est insuffisante. Il y a lieu de désigner une autorité spécifique en tant que responsable de traitement[476].

Enfin, la *transparence* des échanges de données doit être assurée, en mentionnant les informations visées à l'article 9 de la L.V.P. Cette communication devrait se faire « lors du premier contact avec les personnes concernées, par exemple via une fenêtre pop-up »[477].

c. Conclusions

131. Conclusions. Les avis de la Commission rendus ces dernières années en matière d'e-gouvernement soulignent à nouveau combien le principe de légalité, traditionnellement applicable à l'action administrative, est enrichi par les exigences de finalité et de proportionnalité prescrites par le régime de la protection des données à caractère personnel.

472 *Ibidem,* n° 23.
473 Avis n° 03/2010 du 3 février 2010 concernant l'avant-projet de décret modifiant le décret du 19 mars 2004 relatif à la politique sociale locale.
474 *Ibidem,* n° 13.
475 *Ibidem,* n° 14.
476 *Ibidem,* n° 16.
477 *Ibidem,* n° 19.

En effet, la définition claire de la finalité d'un traitement pousse le législateur à réfléchir minutieusement à l'objectif précis de son intervention. Son action doit être guidée par le souci de permettre aux citoyens de savoir ce qu'il advient de leurs données. Par ailleurs, la proportionnalité du traitement et des données impose au pouvoir législatif un examen consciencieux des moyens utilisés et ce, afin de choisir la voie la moins attentatoire aux libertés citoyennes.

3. Cour de Justice de l'Union européenne, Tribunal de première instance et Tribunal de la fonction publique européenne

Claire Gayrel[478]

132. Introduction. La période couverte par cette chronique de jurisprudence en ce qu'elle concerne les juridictions de l'Union européenne est marquée par l'entrée en vigueur, au 1er décembre 2009, du nouveau cadre institutionnel de l'Union tel que défini par le Traité de Lisbonne et par là, de la Charte des droits fondamentaux de l'Union européenne. Il est expressément consacré que cette dernière a la même valeur contraignante que les traités[479]. Cette charte reconnaît en son article 8 le droit à la protection des données à caractère personnel et en son article 7 le droit à la protection de la vie privée, tous deux pertinents pour notre chronique. Nous verrons que les juridictions de l'Union, en particulier la Cour, ont eu l'occasion d'intégrer le nouveau droit fondamental à la protection des données ainsi reconnu dans la Charte dans son raisonnement (a). Après avoir présenté les positions des juridictions quant aux notions de traitement et de données à caractère personnel (b), nous présenterons les arrêts portant sur l'interprétation de dispositions de la directive 95/46[480] (c), de la directive 2002/58[481] (d) et du règlement 45/2001[482] (e), pertinents pour notre chronique. Nous évacuons dans notre introduction la jurisprudence relative à la très controversée directive 2006/24[483] sur la conservation des données de trafic qui, si elle aura généré un certain contentieux, soulève un intérêt limité pour l'objet de cette chronique[484]. Soulignons toutefois la décision de la Cour, saisie d'un recours en annulation de

478 Chercheur au CRIDS.

479 Article 6, § 1er, du Traité sur l'Union européenne.

480 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.* L 281 du 23 novembre1995.

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

482 Règlement CE n° 45/2001 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.* L 8 du 12 janvier 2001.

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

484 Cette directive a généré un contentieux relativement important entre la Commission et plusieurs États membres poursuivis pour manquement à leurs obligations en raison d'un défaut de transposition de l'ensemble ou de certaines des dispositions de la directive 2006/24 en droit national. Voy. C.J.C.E., 26 novembre 2009, *Commission c. Grèce*, C-211/09 ; C.J.C.E., 26 novembre 2009, *Commission c. Irlande*, C-202/09 ; C.J.C.E., *Commission c. Pays-Bas*, C-192/09 (requête abandonnée) ; C.J.C.E., 29 juillet 2010, *Commission c. Autriche*, C-189/09 ; C.J.C.E., 4 février 2010, *Commission c. Suède*, C-185/09 ; C.J.U.E., *Commission c. Luxembourg*, C-394/10.

l'Irlande qui contestait le choix de la base juridique, de considérer que celle-ci était correctement fondée sur l'ex-article 95 CE[485].

a. La protection des données en tant que droit fondamental

133. Un droit fondamental autonome, mais étroitement lié au droit à la protection de la vie privée. L'entrée en vigueur du Traité de Lisbonne et la reconnaissance de la valeur de la Charte des droits fondamentaux de l'Union européenne au rang des sources du droit primaire de l'Union à compter du 1er décembre 2009 a entraîné la reconnaissance de la protection des données à caractère personnel comme droit fondamental par la Cour dans son arrêt *Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen*[486]. Pour rappel, la Charte consacre le droit à la protection des données à caractère personnel dans son article 8, de manière distincte du droit à la protection de la vie privée affirmée en son article 7. La jurisprudence de la Cour rappelle néanmoins le principe de l'article 52, § 3, de la Charte selon lequel « dans la mesure où la charte contient des droits correspondant à des droits garantis par la C.E.D.H., leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention »[487]. Dès lors, les limitations susceptibles d'être légitimement apportées au droit à la protection des données à caractère personnel tel que reconnu à l'article 8 de la Charte doivent correspondre à celles tolérées dans le cadre de l'article 8 relatif à la protection de la vie privée de la Convention européenne des droits de l'homme[488]. Ce qui amène la Cour à préciser que l'article 8, § 1er, relatif au droit fondamental à la protection des données à caractère personnel, est étroitement lié au respect de la vie privée consacré à l'article 7 de la Charte[489]. Elle souligne dans sa jurisprudence que « le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société »[490].

134. L'application du droit fondamental à la protection des données et de la vie privée. Les juridictions européennes montrent des approches différentes lorsqu'il s'agit d'évaluer des ingérences dans le droit à la protection des données et/ou de la vie privée.

485 C.J.C.E. (gr. ch.), 10 février 2009, *Irlande c. Parlement et Conseil*, C-301/06. L'objet du recours en annulation de l'Irlande visait à faire établir que le choix de la base juridique retenue, à savoir l'article 95 CE relatif au rapprochement des dispositions législatives, réglementaires et administratives des États membres ayant pour objet l'établissement et le fonctionnement du marché intérieur, et par là de l'instrument (une directive) était inadéquat, dans la mesure où la conservation des données de trafic aurait pour objectif principal la recherche, la détection et la poursuite d'infractions pénales (ce qui impliquait l'adoption d'une décision-cadre fondée sur une base juridique de l'ancien 3e pilier de l'UE). La Cour a confirmé le choix de la base juridique de l'article 95 CE.

486 C.J.U.E. (gr. ch.), 9 novembre 2011, *Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen*, aff. jointes C-92/09 et C-93/09. Voy. E. Degrave, « Arrêt ''Volker und Markus Schecke et Eifert'' : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.*, 2011, pp. 97-99 et I. Andoulsi, « L'arrêt de la Cour du 9 novembre 2012 dans les affaires jointes *Volker und Markus Schecke GbR et Hartmut Eifert c. Land d'Hessen* : une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles ? », *C.D.E.*, vol. 47, n° 2, 2011, pp. 471-522.

487 Affaire *Volker und Markus Schecke & Eifert*, point 51.

488 *Idem*, point 52.

489 *Idem*, point 47 et C.J.U.E., 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración, del Estado*, aff. jointes C-468/10 et C-469-10, point 41.

490 Affaire *Volker und Markus Schecke & Eifert*, point 48 et C.J.U.E., 5 mai 2011, *Deutsche Telekom AG c. Allemagne*, C-543/09, point 51.

Dans son arrêt *Volker und Markus Schecke & Eifert*, la Cour cherche à appliquer conjointement les articles 7 et 8 de la Charte, en référence à la jurisprudence de la Convention européenne des droits de l'homme relative à l'article 8. Elle affirme alors, en se fondant sur les arrêts *Aman*[491] et *Rotaru*[492] de la Cour de Strasbourg, que la protection offerte par la Charte dans ses articles 7 et 8, s'applique à toute information concernant une personne physique identifiée ou identifiable[493] et que, dès lors, les personnes morales ne peuvent se prévaloir de cette protection sauf dans la mesure où le nom légal de la personne morale identifie une ou plusieurs personnes physiques[494]. Ce qui l'amène à considérer que la publication sur Internet de données nominatives concernant les personnes physiques bénéficiaires d'aides agricoles constitue une ingérence dans leur droit au respect de la vie privée reconnu à l'article 7, et un traitement de données relevant de la protection garantie par l'article 8 de la Charte[495]. Si cette ingérence peut être considérée comme poursuivant un but légitime, à savoir l'accroissement de la transparence de l'utilisation des fonds communautaires de la PAC[496], elle sera finalement jugée disproportionnée par la Cour[497].

Le Tribunal de la fonction publique, dans son arrêt *V c. Parlement* a opté pour une application de l'article 8 de la Convention européenne des droits de l'homme (en sus d'une interprétation des dispositions pertinentes du règlement 45/2001, voy. *infra*). Le litige soulevait la question de la légalité du transfert de la Commission au Parlement d'un dossier médical archivé concernant une candidate à un poste d'agent contractuel au sein de la seconde institution, et écartée du recrutement sur le fondement de ce dossier médical pour raisons d'inaptitude sans que de nouveaux examens médicaux n'aient été accomplis[498]. Le Tribunal y rappelle la jurisprudence de la Convention européenne des droits de l'homme selon laquelle la vie privée comporte le droit de tenir son état de santé secret[499]. Il considère que le transfert entre institutions de données relatives à la santé d'une personne constitue une ingérence dans sa vie privée et ce, quelle que soit l'utilisation ultérieure des données communiquées[500]. Si le Tribunal semble exprimer des doutes sur le fait qu'une telle ingérence soit valablement « prévue par la loi » compte tenu des termes très généraux en lesquels sont prévus les transferts entre institutions[501], il poursuivra son raisonnement en affirmant que la réalisation d'un examen d'embauche sert bien un intérêt légitime des institutions

491 Cour eur. D.H., 16 février 2000, *Amann c. Suisse*.
492 Cour eur. D.H., 4 mai 2000, *Rotaru c. Roumanie*.
493 Affaire *Volker und Markus Schecke & Eifert*, point 52.
494 *Idem*, point 53.
495 *Idem*, points 58 et 60.
496 *Idem*, point 71.
497 *Idem*, point 86.
498 T.F.P., 5 juillet 2011, *V c. Parlement*, F-46/09 ; J.-M. Van Gyseghem et F. Omrani, « Quand le transfert des données ''santé'' est illégal », note sous Tribunal de la fonction publique de l'Union européenne (1re ch.), 7 juillet 2011, *R.D.T.I.*, n° 45/2011, pp. 121-149.
499 *Idem*, point 111.
500 *Idem*, point 112.
501 En effet, tandis que la condition de légalité du transfert est supposée reposer sur l'article 7 du règlement 45/2001, le Tribunal soutient au point 117 que « l'article 7 du règlement n° 45/2001 prévoit dans des termes très généraux que les transferts de données entre institutions ne sont possibles que si les données communiquées ''sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire'', et que ''la question se pose de savoir si cet article est libellé avec suffisamment de précision pour permettre aux destinataires de la loi de régler leur conduite et répond à l'exigence de prévisibilité dégagée par la jurisprudence de la Cour européenne des droits de l'homme'' ». Voy. *infra* nos développements sur le raisonnement du Tribunal dans cette affaire quant à la violation des articles 6 et 7 du règlement 45/2001.

de l'Union susceptible de justifier une telle ingérence[502]. En revanche, compte tenu du caractère extrêmement intime et sensible des données à caractère médical[503], il juge en l'espèce que « cet intérêt ne justifie pas que l'on procède à un transfert de données médicales d'une institution à une autre sans le consentement de l'intéressé »[504], car le Parlement aurait pu satisfaire sa mission dans des conditions moins attentatoires.

Enfin, dans l'affaire *Scarlet* commentée ailleurs dans cette chronique[505], la Cour ne fera pas application du droit à la protection des données de la Charte, se contentant d'affirmer qu'un système de filtrage des communications électroniques aux fins d'empêcher l'échange de fichiers portant atteinte aux droits d'auteurs *est susceptible de porter atteinte* à ce droit fondamental protégé en son article 8[506].

b. Notions de données à caractère personnel et de traitement

135. Données à caractère personnel. Conduites à interpréter des dispositions de la directive 95/46 ou du règlement 45/2001, les juridictions de l'Union ont eu à vérifier au préalable, de manière plus ou moins évidente, si elles se trouvaient effectivement en présence d'un traitement de données à caractère personnel soumis auxdites réglementations.

C'est ainsi qu'elles ont eu l'occasion de confirmer que les noms et prénoms[507] peuvent être considérés comme des données à caractère personnel, mais aussi l'adresse[508], et que la communication de telles données constitue un traitement[509]. Le Tribunal de première instance a lui aussi établi, au soutien de la Commission européenne, que les noms et prénoms des fonctionnaires européens ou des personnes figurant sur les listes de réserve des concours généraux européens constituaient des données à caractère personnel[510], au détriment de la position du requérant qui soutenait que l'information selon laquelle une personne est fonctionnaire ne peut pas être considérée comme relevant de sa vie privée[511]. La Cour a établi que la publication de données à caractère personnel sur Internet, en l'espèce les noms des bénéficiaires d'aides agricoles au titre de la PAC, constituait bien un traitement de données[512], mais aussi la transmission par un exploitant de réseau de télécommunications attribuant des numéros de téléphone de données à caractère personnel concernant ses abonnés à une entreprise tierce fournisseur de services de renseignements téléphoniques accessibles au public[513]. Conduite à interpréter l'étendue du droit d'accès des individus aux informations concernant les destinataires de données à caractère personnel en cas de communication (voy. *infra*), la Cour a explicité que l'information sur les destinataires

502 *Idem*, point 120.
503 *Idem*, point 123.
504 *Idem*, point 125.
505 Voy. § 31 et § 51.
506 C.J.U.E., 24 novembre 2011, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, point 50.
507 C.J.U.E. (gr. ch.), 29 juin 2010, *Commission c. The Bavarian Lager Co. Ltd*, C-28/08, point 86.
508 C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, C-553/07, point 42.
509 Affaire *The Bavarian Lager Co.*, point 86.
510 T.P.I., 7 juillet 2011, *Gregorio Valero Jordana c. Commission*, T-161/04, point 91.
511 *Idem*, point 60.
512 Affaire *Volker und Markus Schecke & Eifert*, point 60.
513 Affaire *Deutsche Telekom*, point 53.

ou les catégories de destinataires auxquels des données à caractère personnel sont communiquées ainsi que le contenu de ces dernières sont à distinguer des données à caractère personnel de base traitées, et constituent des informations relatives au traitement[514]. Enfin, il faut souligner que bien que la Cour n'ait pas procédé à l'application des articles 7 et 8 de la Charte dans l'affaire *Scarlet* (voy. *supra*), elle a néanmoins procédé à la reconnaissance des adresses IP des utilisateurs à l'origine de l'envoi de contenus illicites sur le réseau, comme données à caractère personnel relatives à ces utilisateurs, dans la mesure où leur collecte et traitement visent à les identifier précisément[515].

c. La directive 95/46 « protection des données à caractère personnel »

136. Introduction. Plusieurs arrêts ont apporté des interprétations éclairantes de la directive 95/46 sur la protection des données à caractère personnel, notamment en ce qui concerne l'intérêt légitime du responsable de traitement comme base de légitimité à un traitement, la portée dans le temps du droit d'accès des individus, la portée des obligations administratives du responsable du traitement et enfin concernant le principe d'indépendance des autorités nationales de contrôle. Notons que la Cour a eu l'occasion de rappeler qu'« il incombe aux États membres, lors de la transposition de la directive 95/46, de veiller à se fonder sur une interprétation de cette dernière qui leur permette d'assurer un juste équilibre entre les différents droits et libertés fondamentaux protégés par l'ordre juridique de l'Union »[516].

137. Intérêt légitime du responsable de traitement. Dans l'affaire *ASNEF*, il s'agissait pour la Cour de déterminer si l'article 7, sous f) de la directive relatif à la nécessité d'un traitement sur le fondement de l'intérêt légitime du responsable du traitement[517] s'opposait à l'exigence de la réglementation espagnole selon laquelle une telle base de légitimité ne puisse jouer que pour des données figurant dans des sources accessibles au public, telles que définies dans le droit national.

La Cour a tout d'abord considéré que l'article 7 de la directive 95/46 prévoyait « une liste exhaustive et limitative des cas dans lesquels un traitement de données peut être considéré comme licite »[518], excluant dès lors la possibilité pour les États membres de prévoir en dehors des cas énumérés, de nouvelles bases de légitimité, ou bien d'en modifier la portée en prévoyant des exigences supplémentaires[519]. Elle reconnaît néanmoins que l'article 7, sous f) de la directive qui prévoit deux conditions cumulatives à la nécessité du traitement, à savoir la réalisation d'un intérêt légitime du responsable de traitement et le respect des droits et libertés fondamentaux de la personne concernée, appelle à une pondération des droits et intérêts en cause[520]. Si la Cour admet que les États membres disposent d'une marge d'appréciation pour l'établissement de prin-

514 Affaire *Rijkeboer*, point 43.
515 Affaire *Scarlet*, point 51.
516 Affaire *ASNEF*, et C.J.C.E. (gr. ch.), 29 janvier 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, C-275/06, point 68.
517 Cet article dispose que le traitement de données à caractère personnel est licite s'« il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée […] ».
518 Affaire *ASNEF*, point 30.
519 *Idem*, point 32.
520 *Idem*, point 40.

cipes directeurs utiles à ladite pondération[521], et que « la gravité de l'atteinte aux droits fondamentaux de la personne concernée par ledit traitement peut varier en fonction du fait de savoir si les données en cause figurent déjà, ou non, dans des sources accessibles au public »[522], l'article 7, sous f) « s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées »[523], en l'espèce des données qui ne figureraient pas dans des sources accessibles au public. Enfin, la Cour considère que l'article 7, sous f) est une disposition qui remplit les conditions de précision pour lui reconnaître un effet direct[524].

138. Droit d'accès des individus dans le temps. Dans l'affaire *Rijkeboer*, la Cour a eu l'occasion d'apporter une interprétation tout à fait éclairante de la portée dans le temps du droit d'accès consacré à l'article 12, sous a) de la directive, et plus particulièrement du droit d'accès aux informations portant sur *les destinataires ou les catégories de destinataires* auxquels les données à caractère personnel de l'individu ont été communiquées, appelées en langage informatique *log files*. La Cour a affirmé que le droit au respect de la vie privée « implique que la personne concernée puisse s'assurer que […] les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés »[525]. Contre les avis exprimés par le requérant au principal devant le Conseil d'État des Pays-Bas et de plusieurs États membres, la Cour a considéré que pour assurer l'effet utile des autres droits octroyés par la directive aux individus, à savoir ses droits de rectification, d'opposition et de recours en cas de dommage[526], le droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi que sur le contenu des données communiquées « doit nécessairement concerner le passé »[527]. Aux fins de déterminer l'étendue de ce droit d'accès dans le passé, et dès lors de fixer la durée de conservation des informations portant sur les destinataires, les États membres sont tenus de prendre en considération plusieurs paramètres : la durée de conservation des données de base[528] ; les dispositions de droit national relatives aux délais de recours ; la nature plus ou moins sensible des données ; le nombre et la fréquence des communications à des destinataires[529] ; et plus généralement le caractère proportionné de la charge de l'obligation de conservation pour les responsables de traitement[530]. En l'espèce, la Cour a jugé qu'« [u]ne réglementation nationale limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation

521 *Idem*, point 46.
522 *Idem*, point 44.
523 *Idem*, points 48-49.
524 *Idem*, point 55.
525 Affaire *Rijkeboer*, point 49.
526 Ces droits sont consacrés aux articles 12, sous b) et c), 14, 22 et 23.
527 Affaire *Rijkeboer*, point 54. Voy. aussi C. de Terwangne, note sous C.J.U.E. (3e ch.), 7 mai 2009, *R.D.T.I.*, n° 43/2011, pp. 65-81.
528 Affaire *Rijkeboer*, point 58.
529 *Idem*, point 63.
530 *Idem*, points 62-63.

plus longue de cette information constituerait une charge excessive pour le responsable du traitement »[531].

139. Obligations administratives du responsable de traitement. La Cour a jugé que l'article 18, § 2, de la directive 95/46, qui prévoit la possibilité pour le responsable du traitement de voir ses obligations administratives de notification simplifiées lorsqu'il nomme un détaché à la protection des données, n'impose aucune obligation à ce dernier de tenir un registre contenant les informations relatives au traitement préalablement à la mise en œuvre dudit traitement[532]. Elle a en outre précisé que « la directive 95/46 ne soumet pas les traitements de données à caractère personnel à un contrôle préalable généralisé »[533], ne prévoyant la possibilité pour les États membres de procéder à des examens avant leur mise en œuvre que des *traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées* en application de l'article 20, § 1er.

140. Indépendance des autorités de contrôle. Réunie en grande chambre, la Cour était saisie d'une requête de la Commission européenne contre l'Allemagne visant à établir le manquement de cet État à son obligation au titre de l'article 28 de la directive 95/46 relatif à l'indépendance des autorités de contrôle[534]. Il s'agissait de déterminer si les autorités de contrôle du secteur non public instituées au niveau des Länders et soumises à une tutelle exercée par l'État étaient compatibles avec la directive 95/46 qui prévoit que les autorités de contrôle (sans distinction du secteur public ou non public), « exercent en toute indépendance les missions dont elles sont investies ». La Cour étend la question de l'indépendance des autorités de contrôle de la directive 95/46 au règlement 45/2001, établissant que : « [l]'article 44 du règlement 45/2001 et l'article 28 de la directive 95/46 sont fondés sur le même concept général, il convient d'interpréter ces deux dispositions de manière homogène, de sorte que non seulement l'indépendance du CEPD[535], mais aussi celle des autorités nationales, impliquent l'absence de toute instruction relative à l'exercice de leurs missions »[536]. Elle considère, contre la position soutenue par l'Allemagne, que « rien n'indique que l'exigence d'indépendance concerne exclusivement la relation entre les autorités de contrôle et les organismes soumis à leur contrôle »[537], jugeant alors que « cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte […] »[538]. Ce qui lui permet de conclure que l'Allemagne a manqué à son obligation en vertu de l'article 29 de la directive 95/46 en soumettant les autorités de contrôle du secteur non public à la tutelle de l'État[539].

531 *Idem*, point 66.
532 Affaire *Volker und Markus Schecke & Eifert*, point 101.
533 *Idem*, point 104.
534 C.J.U.E. (gr. ch.), 9 mars 2010, *Commission c. Allemagne*, C-518/07.
535 Contrôleur européen de protection des données.
536 C.J.U.E. (gr. ch.), 9 mars 2010, *Commission c. Allemagne*, C-518/07, point 28.
537 *Idem*, point 19.
538 *Idem*, point 30.
539 *Idem*, point 56.

d. Directive 2002/58 « vie privée et communications électroniques »

141. Limitations à la confidentialité des communications. La Cour a eu l'occasion de confirmer, dans l'affaire *LSG Gesellschaft*[540], sa jurisprudence établie dans l'affaire *Promusicae* selon laquelle « le droit communautaire, notamment l'article 8, paragraphe 3, de la directive 2004/48[541], lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58, ne s'oppose pas à ce que les États membres établissent une obligation de transmission à des personnes privées tierces de données à caractère personnel relatives au trafic pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur »[542]. Comme dans l'affaire *Promusicae*, la Cour demeure réticente à établir le juste équilibre entre confidentialité des communications d'un côté, protection des droits d'auteur de l'autre, renvoyant aux États membres le soin de veiller à se fonder sur une interprétation du droit communautaire qui permette d'assurer ce juste équilibre et ce, de manière conforme aux droits fondamentaux et autres principes généraux du droit communautaire, tels que le principe de proportionnalité.

142. Publication d'annuaires publics d'abonnés. Dans l'affaire *Deutsche Telekom*, il s'agissait pour la Cour de se prononcer sur l'interprétation de l'article 12 de la directive 2002/58, et en particulier son § 2 relatif à l'exigence du consentement des abonnés à des services de télécommunications pour la publication des données à caractère personnel les concernant dans les annuaires publics[543]. La Cour a déterminé qu'« il ressort d'une interprétation contextuelle et systématique de l'article 12 que le consentement porte sur la finalité de la publication des données à caractère personnel dans un annuaire public et non sur l'identité d'un fournisseur d'annuaire en particulier »[544]. Dès lors, le consentement dûment informé des abonnés à la publication des données le concernant dans un annuaire public « s'étend ainsi à tout traitement ultérieur desdites données par des entreprises tierces actives sur le marché des services de renseignements téléphoniques accessibles au public et d'annuaire, pour autant que de tels traitements poursuivent cette même finalité »[545]. La transmission des données en question entre entreprises aux fins de publication d'annuaires publics ne requiert pas l'obtention d'un nouveau consentement de la part des abonnés et ne porte pas atteinte à la substance même du droit à la protection des données à caractère personnel tel que reconnu à l'article 8 de la Charte[546].

e. Règlement 45/2001 sur la protection des données traitées par les institutions de l'Union

143. Exigence de nécessité des transferts de données sensibles entre institutions. Outre l'examen de légalité du transfert entre institutions du dossier médical de la requérante au principal au regard de l'article 8 de la Convention européenne des droits de l'homme (voy. *supra*), le Tribunal de la fonction publique a, dans l'affaire *V c. Parlement*, examiné extensivement la légalité de ce transfert au regard du règlement 45/2001. Il y procède à une lecture et interprétation conjointe des

540 C.J.C.E., 19 février 2009, *LSG-Gesellschaft c. Tele2 Telecommunication GmbH*, C-557/07.

541 Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, *J.O.* L 195 du 2 juin 2004.

542 Affaire *LSG-Gesellschaft c. Tele2 Telecommunication GmbH*, point 29 ; affaire *Promusicae*, point 70.

543 Affaire *Deutsche Telekom*.

544 *Idem*, point 61.

545 *Idem*, point 65.

546 *Idem*, point 66.

principes posés aux articles 7[547] et 10, § 2, b)[548]. Admettant qu'un transfert de données médicales entre deux institutions, en l'espèce de la Commission au Parlement, à des fins d'embauche peut être analysé comme une « obligation en matière de droit du travail » au sens de l'article 10, § 2, b), à laquelle le Parlement, en tant qu'employeur et responsable du traitement serait soumis, le Tribunal considère néanmoins que la *nécessité* du transfert aux fins de respecter cette obligation n'est pas suffisamment établie, notamment en raison de l'existence de mesures moins attentatoires à la vie privée[549] comme il s'est attaché à le démontrer dans son raisonnement fondé sur l'article 8 de la Convention européenne des droits de l'homme. Dès lors, si un tel transfert ne peut être considéré comme nécessaire au sens de l'article 10 du règlement 45/2001, il ne peut pas l'être non plus aux fins de l'exécution légitime de missions relevant de la compétence du Parlement, à savoir l'examen de l'aptitude physique à l'embauche de la requérante, fondé sur l'article 7[550].

144. Protection des données à caractère personnel et droit d'accès aux documents des institutions. La question de l'équilibre entre la protection de la vie privée et des données à caractère personnel et la transparence administrative, en particulier le droit d'accès aux documents des institutions de l'Union européenne et par là de l'articulation des règlements 45/2001 et 1049/2001[551] posée par l'article 4, § 1er, sous b)[552], de ce dernier, a été soulevée devant les juridictions européennes. Elles ont tout d'abord clairement affirmé que si « les règlements n° 45/2001 et n° 1049/2001 […] ne comportent pas de dispositions prévoyant expressément la primauté de l'un des règlements sur l'autre »[553], « lorsqu'une demande fondée sur le règlement n° 1049/2001 vise à obtenir l'accès à des documents comprenant des données à caractère personnel, les dispositions du règlement n° 45/2001 deviennent intégralement applicables »[554]. Le Tribunal a en particulier jugé qu'en raison du lien explicite entre le règlement 1049/2001 et le règlement 45/2001 établi par l'article 4, § 1er, sous b), du premier règlement, la Commission est tenue d'appliquer le second règlement lorsqu'une demande d'accès à des documents comprend des données à caractère personnel et ce, même si le demandeur a fondé sa demande d'accès uniquement sur le règlement 1049/2001. Cette position répond « aux exigences d'une bonne administration »[555]. C'est ce que la Commission européenne avait, à bon droit, fait pour la demande d'accès introduite par la société *Bavarian Lager* qui avait sollicité l'obtention d'un procès-verbal de réunion aux fins de connaître l'identité et les opinions exprimées par les participants sur le fondement du règlement 1049/2001. La Cour a jugé qu'en diffusant la version expurgée des cinq noms de parti-

547 « […] 1) Les données à caractère personnel ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire ».

548 Cet article prévoit la possibilité de traiter des données sensibles, dont les données à caractère médical lorsque « le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail […] ».

549 *Idem*, point 139.

550 *Idem*, point 141.

551 Règlement n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, *J.O.* L 145, 31 mai 2001.

552 « Les institutions refusent l'accès à un document dans le cas où la divulgation porterait atteinte à la protection : […] b) de la vie privée et de l'intégrité de l'individu, notamment en conformité avec la législation communautaire relative à la protection des données à caractère personnel ».

553 Affaire *The Bavarian Lager Co.*, point 56.

554 Affaire *The Bavarian Lager Co.*, point 36 et affaire *Valero Jordana*, point 88.

555 Affaire *Valero Jordana*, points 100-102.

cipants n'ayant pas donné leur consentement, la Commission « s'est soumise à suffisance à son obligation de transparence »[556]. En outre, la Commission s'est correctement conformée au droit communautaire en appliquant l'article 8, sous b), du règlement 45/2001[557] exigeant que *Bavarian Lager* fournisse une justification expresse et légitime démontrant la nécessité du transfert des données personnelles en question en l'absence de consentement des participants concernés[558].

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

Jean Herveg[559]

145. Introduction. Les droits garantis par l'article 8 sont éminemment personnels et non transférables[560].

146. Obligations positives visant à assurer l'effectivité du droit au respect de la vie privée. La Cour a mis l'accent sur l'importance d'une approche prudente dans les obligations positives de l'État de protéger la vie privée en général ainsi que sur le besoin de reconnaître la diversité des méthodes possibles pour y parvenir. La nature de l'obligation dépend de l'aspect de la vie privée qui est concerné et le choix des mesures relève de la marge d'appréciation de l'État contractant. La Cour considère que l'exigence minimale consiste en la mise en place d'un système juridique effectif qui protège les droits qui tombent dans la notion de « vie privée »[561]. Mais, lorsqu'un aspect important de l'existence d'une personne ou de son identité est en jeu, la marge d'appréciation de l'État est restreinte[562].

147. Vie privée et activités professionnelles. Il n'existe aucune raison de principe de considérer que la « vie privée » exclurait les activités professionnelles. Ainsi, des restrictions apportées à la vie professionnelle peuvent tomber sous le coup de l'article 8 lorsqu'elles se répercutent dans la façon dont l'individu forge son identité sociale par le développement de relations avec ses semblables. La Cour ajoute que c'est dans le cadre de leur travail que la majorité des gens ont beaucoup, voire le maximum, d'occasions de resserrer leurs liens avec le monde extérieur[563].

148. Droit à l'autodétermination. Il est acquis depuis plusieurs années que la notion de « vie privée » englobe, entre autres, le droit à l'autodétermination[564]. Dans la société de l'information, ce

556 Affaire *The Bavarian Lager Co.*, point 76.

557 « Sans préjudice des articles 4, 5, 6 et 10, les données à caractère personnel ne sont transférées à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46 […] que si : b) le destinataire démontre la nécessité de leur transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes de la personne concernée ».

558 *Ibidem*, point 77.

559 Chargé d'enseignement à la Faculté de Droit de Namur (MC Droit de l'Internet). Directeur de Recherche au CRIDS. Avocat au barreau de Bruxelles.

560 Cour eur. D.H. (5e sect.), décision du 29 juin 2010, *Mitev c. Bulgarie*, n° 42758/07. Voy. aussi la décision du 21 septembre 2010 en cause de *Todorov c. Bulgarie*, n° 11.571/04.

561 Voy. Cour eur. D.H., arrêt du 28 avril 2009, *Karako c. Hongrie*, n° 39311/05, § 19 ; arrêt du 30 mars 2010, *Petrenco c. Moldavie*, n° 20928/05, § 54 ; arrêt du 10 mai 2011, *Mosley c. Royaume-Uni*, n° 48009/08, § 107.

562 Cour eur. D.H., arrêt du 1er avril 2010, *S.H. et autres c. Autriche*, n° 57813/00, § 93.

563 Cour eur. D.H., arrêt du 19 octobre 2010, *Ozpinar c. Turquie*, n° 20.999/04, § 46.

564 Voy. Cour eur. D.H., arrêt du 3 novembre 2011, *S.H. et autres c. Autriche*, n° 57.813/00, § 80. Dans son arrêt *Schlumpf c. Suisse* du 8 janvier 2009 (n° 29002/06, § 100), la Cour a affirmé qu'elle n'avait jamais établi que l'article 8 comporterait

droit fait inévitablement penser à la maîtrise de l'individu sur les informations qui le concernent (la fameuse « autodétermination informationnelle »). Mais, ce droit peut aussi trouver à s'exprimer autrement, notamment dans le cadre des obligations positives à charge des États d'assurer l'effectivité du droit au respect de la vie privée et qui concerneraient l'individu dans la société de l'information, en ce compris dans les mondes virtuels. Ceci renvoie, par exemple, au phénomène du profilage et des « réseaux sociaux » ou au « droit à l'oubli ».

149. Identité et intégrité personnelles. La notion de « vie privée » inclut l'identité personnelle et la protection de la vie privée s'étend à la protection de l'intégrité personnelle, cette approche étant le résultat de la large interprétation donnée à l'article 8 pour inclure les notions d'intégrité personnelle et de libre développement de la personnalité[565]. La notion de « vie privée » peut aussi englober des aspects de l'identité physique et sociale d'un individu. De même, l'identité sexuelle et le nom relèvent de la sphère personnelle protégée par l'article 8[566]. À l'instar d'aspects comme le nom, le sexe, la religion et l'orientation sexuelle, l'identité ethnique d'une personne constitue un élément essentiel de sa vie privée et de son identité[567].

L'article 8 de la Convention ne contient pas de disposition explicite en matière de nom, mais en tant que moyen d'identification personnelle et de rattachement à une famille, le nom d'un individu n'en concerne pas moins la vie privée et familiale de celui-ci. Que l'État et la société aient intérêt à en réglementer l'usage ne suffit pas pour exclure la question du nom d'un individu du domaine de la vie privée et familiale, conçue comme englobant, dans une certaine mesure, le droit pour cet individu de nouer des relations avec ses semblables[568]. Il faut retenir que le nom, en tant qu'élément d'individualisation principal d'une personne au sein de la société, appartient au noyau dur des considérations relatives au droit au respect de la vie privée et familiale[569].

150. Publication d'avis de recherche. Comme la notion de « vie privée » comprend des éléments relatifs au droit à l'image, la publication du portrait d'une personne erronément recherchée pour meurtre, sans son consentement, constitue une ingérence dans l'exercice de son droit au respect de la vie privée. La gravité de l'ingérence s'apprécie par rapport à la volonté de rendre la photographie accessible au plus large public, au procédé utilisé pour en assurer la diffusion, et à l'objectif poursuivi. Dans l'affaire *Nikolaishvili c. Georgie*, la Cour a tenu compte du fait que la publication avait porté atteinte gratuitement à la réputation du requérant alors que celle-ci fait part de son identité sociale et de son intégrité psychologique qui toutes deux tombent dans le champ de la vie privée. Le respect de la vie privée impose à l'État de prendre, aussi vite que possible, toutes les mesures nécessaires afin de remédier à « toute divulgation de nature privée incompatible avec l'article 8 ».

---

un droit à l'autodétermination en tant que tel. Pourtant, elle avait déjà affirmé l'existence de ce droit dans au moins quatre décisions antérieures (voy. les références reprises dans la précédente chronique, p. 104, n° 170).

565 Cour eur. D.H., arrêt du 28 avril 2009, *Karako c. Hongrie*, n° 39311/05, § 21.

566 Cour eur. D.H., arrêt du 8 janvier 2009, *Schlumpf c. Suisse*, n° 29002/06, § 100.

567 Cour eur. D.H., arrêt du 27 avril 2010, *Ciubotaru c. Moldavie*, n° 27138/04, § 53.

568 Cour eur. D.H., arrêt du 9 novembre 2010, *Losonci Rose & Rose c. Suisse*, n° 664/06, § 26.

569 *Ibidem*, § 51.

Une fois que la divulgation a eu lieu en violation de l'article 8, l'obligation positive inhérente au respect de la vie privée induit une obligation de mener une enquête dans le but de remédier à la situation autant que faire se peut[570].

Il y a ingérence dans le droit au respect de la vie privée lorsque des images et des photographies d'un individu sont enregistrées, sans son consentement, par des journalistes au siège de la police à la demande de cette dernière, afin de les diffuser dans les médias le jour même où des poursuites sont entamées contre lui[571]. Dans la mesure où l'individu n'était pas un fugitif, puisqu'il se trouvait en garde à vue dans les locaux de la police, et que le procès pénal public n'avait pas encore débuté, la diffusion de ces images, qui n'avaient pas de valeur informationnelle, ne pouvait pas viser au respect des intérêts de la justice, comme assurer sa comparution au procès ou la prévention d'infractions pénales, l'acte d'accusation n'ayant pas encore été rédigé[572].

151. Prise de photographies. L'image d'un individu est un des attributs principaux de sa personnalité du fait qu'elle dégage son originalité et lui permet de se différencier de ses congénères. Le droit de l'individu à la protection de son image constitue ainsi un des composants essentiels de son épanouissement personnel et présuppose principalement la maîtrise de celle-ci par lui. Si la maîtrise de son image implique, dans la plupart des cas, la possibilité, pour l'individu, de refuser la diffusion de son image, elle comprend, en même temps, le droit de s'opposer à la captation, la conservation et la reproduction de celle-ci par autrui. Le fait que l'individu soit une personne publique ou un personnage d'actualité peut justifier, dans certaines circonstances, la captation de son image à son insu et sans son consentement, en vue de servir l'intérêt général[573].

Dans le cadre d'une prise en charge hospitalière où des abus sexuels étaient suspectés à charge d'un père mais de manière erronée comme il sera établi ultérieurement, la décision de quand même réaliser une analyse de sang et de prendre une photographie de parties intimes de son enfant mineure contre les instructions expresses des deux parents, alors qu'ils étaient absents, constitue une ingérence dans le droit au respect de la vie privée de l'enfant et en particulier dans son droit à l'intégrité physique[574]. Lorsqu'il s'agit d'un patient mineur, seule la personne investie de l'autorité parentale est habilitée à autoriser toute intervention médicale[575]. Face au refus des parents d'autoriser un acte médical, seule l'urgence est de nature à justifier la décision de réaliser l'analyse de sang et de prendre les photographies[576].

152. Droit d'accès et droit de copie. S'agissant de l'accès à des fichiers personnels détenus par des pouvoirs publics, en dehors du contexte des renseignements sensibles pour la sécurité nationale, les individus ont un intérêt primordial à obtenir les renseignements pour connaître et comprendre leur enfance et leurs années de formation ou pour retracer leur identité personnelle, s'agissant en particulier de leur filiation naturelle ou de renseignements sur les risques pour la santé auxquels ils ont été exposés. Dans ce contexte, les autorités doivent offrir aux intéressés

570 Cour eur. D.H., arrêt du 13 janvier 2009, *G. Nikolaishvili c. Georgie*, n° 37048/04, spéc. §§ 121, 122 et 130.
571 Cour eur. D.H., arrêt du 24 février 2009, *Toma c. Roumanie*, n° 42716/02, § 91.
572 *Ibidem*, § 92.
573 Cour eur. D.H., arrêt du 15 janvier 2009, *Reklos et Davourlis c. Grèce*, n° 1234/05.
574 Cour eur. D.H., arrêt du 23 mars 2010, *M.A.K. et R.K. c. Royaume-Uni*, n° 45901/05 et 40146/06, § 75.
575 *Ibidem*, § 77.
576 *Ibidem*, § 79.

une « procédure effective et accessible » qui leur permette d'avoir accès à « l'ensemble des informations pertinentes et appropriées ». Le grand âge d'un individu accentue l'urgence à pouvoir retracer son parcours personnel[577].

Dans le cadre d'une procédure d'attribution de la garde d'un enfant suite à la séparation de ses parents, le père souhaitait obtenir une copie d'un rapport établi par la Société pour la protection de l'enfance. Celle-ci a refusé de satisfaire à sa demande, le rapport étant confidentiel et destiné à la seule attention de la juridiction chargée de trancher le litige. Cette juridiction a rejeté sa demande d'accès excipant d'une absence d'intérêt légitime à prendre connaissance d'informations concernant les données personnelles d'un mineur. La Cour a considéré que les informations contenues dans ce rapport étaient pertinentes pour le requérant et sa relation avec son fils, notant que si la juridiction avait estimé que l'intérêt de l'enfant imposait de ne pas l'éloigner de la mère, elle avait reconnu que le père faisait preuve d'une grande affection envers son fils démontrée d'ailleurs par ses efforts persistants pour en obtenir la garde. La Cour a, dès lors, considéré que la communication du rapport lui aurait permis de prendre connaissance d'éventuels points négatifs contenus dans celui-ci et qui ont pu influencer la décision du tribunal et, le cas échéant, de les prendre en compte pour l'avenir afin d'améliorer sa relation avec son fils.

De plus, elle a noté que le requérant avait participé à l'élaboration du rapport et qu'il était donc légitime qu'il puisse connaître la manière dont les informations qu'il avait fournies avaient été analysées et prises en compte par la Société pour la protection de l'enfance. Par voie de conséquence, la Cour a jugé que le refus non motivé des autorités à consentir à la divulgation du rapport après la fin de la procédure s'analysait en une méconnaissance de l'obligation positive d'assurer le respect effectif du droit du requérant à sa vie privée et familiale, soulignant qu'il appartenait aux autorités nationales de démontrer l'existence de raisons impérieuses justifiant la non-divulgation au requérant d'un rapport contenant des informations personnelles le concernant directement[578].

Les informations personnelles relatives à un patient relèvent incontestablement de sa vie privée et la question de l'accès du patient à ces informations relève de l'article 8[579]. La Cour a eu l'occasion de préciser que le droit d'un individu à accéder à des informations relatives à sa santé tombait dans la notion de vie privée[580]. De même, l'exercice du droit à un accès effectif à l'information relative la santé et à la possibilité de procréer est lié en tant que tel à la vie privée et familiale au sens de l'article 8[581]. Pour rappel, l'accès des individus à des informations leur permettant d'évaluer les risques sanitaires auxquels ils ont été ou sont exposés entre dans le champ d'application de l'article 8.1[582].

Un détenu possède un intérêt à obtenir une copie du rapport établi après son examen médical à la clinique de la prison, ainsi que la page pertinente du registre relative à son admission dans cette clinique afin qu'il puisse être impliqué correctement dans le choix des soins de santé à lui prodiguer[583].

577 Cour eur. D.H., arrêt du 27 octobre 2009, *Haralambie c. Roumanie*, n° 21737/03, §§ 85-86, 93 et s.
578 Cour eur. D.H., arrêt du 15 octobre 2009, *Tsourlakis c. Grèce*, n° 50796/07, §§ 39-40 et 43-44.
579 Cour eur. D.H., arrêt du 20 janvier 2009, *Uslu c. Turquie (n° 2)*, n° 23815/04, § 22.
580 Cour eur. D.H., arrêt du 26 mai 2011, *R.R. c. Pologne*, n° 27.617/04, § 197.
581 Cour eur. D.H., arrêt du 28 avril 2009, *K.H. et autres c. Slovaquie*, n° 32881/04, § 44.
582 Cour eur. D.H., décision du 12 octobre 2010, *Dossi & autres c. Italie*, n° 26.053/07.
583 Cour eur. D.H., arrêt du 20 janvier 2009, *Uslu c. Turquie (n° 2)*, n° 23815/04, § 25.

Lorsque des données à caractère personnel sont en cause, les obligations positives tirées de l'article 8 imposent, notamment, la mise à disposition de copies du dossier de données au profit de la personne concernée. Il peut revenir au détenteur du dossier de déterminer les modalités de reproduction du dossier et de dire le coût qui doit en être supporté par la personne concernée. Toutefois, celle-ci ne devrait pas être obligée de justifier sa demande à obtenir une copie du dossier. C'est plutôt aux autorités de prouver qu'il existerait des raisons impérieuses de s'y opposer. À ce sujet, la Cour a indiqué qu'elle ne voyait pas comment la personne pourrait abuser des informations qui la concernent en faisant des photocopies des documents pertinents de son dossier médical, surtout lorsqu'elle avait déjà eu accès à la totalité de son contenu[584].

Le risque d'un abus par des tiers peut être évité autrement que par le refus de délivrer des copies du dossier médical à la personne concernée. Ainsi, la communication ou la divulgation de données à caractère personnel relatives à la santé, incompatible avec les garanties de l'article 8, peut être évitée en incorporant dans le droit national des mesures appropriées visant à limiter strictement les circonstances dans lesquelles ces données peuvent être divulguées et les personnes susceptibles de pouvoir accéder aux dossiers[585].

Comme la condition et la santé d'un fœtus durant la vie privée sont des éléments de la santé de la femme enceinte, l'exercice effectif du droit d'accéder à des informations relatives à sa santé est souvent décisif pour l'exercice de l'autonomie personnelle (aussi couverte par l'article 8) en ce qu'il permet, sur la base de ces informations, de prendre des décisions à propos d'événements futurs relatifs à la qualité de vie de l'individu (comme par exemple refuser de consentir à un traitement médical ou demander de recevoir un traitement médical). L'importance d'accéder au moment adéquat à des informations relatives à la santé d'une personne est d'autant plus grande quand des évolutions rapides interviennent dans la condition de cette personne et que sa capacité à prendre des décisions pertinentes s'en trouve réduite. C'est encore plus vrai lorsque l'accès à des informations sur la santé de la mère et du fœtus est directement pertinent pour l'exercice de l'autonomie personnelle quand la législation autorise l'avortement dans certaines situations. Ainsi, lorsque la législation nationale autorise l'avortement en cas de malformation fœtale, il doit y avoir un cadre légal et procédural qui garantisse que des informations pertinentes, complètes et fiables sur la santé du fœtus soient disponibles à la femme enceinte[586].

153. Écoutes téléphoniques. Les communications par courrier, téléphone et par e-mail, en ce compris celles intervenues dans le contexte de négociations professionnelles, sont couvertes par la notion de « vie privée » et de « correspondance » de l'article 8.1[587]. Dès lors, leur interception, la mémorisation des données ainsi obtenues et leur éventuelle utilisation dans le cadre de pour-

584 Cour eur. D.H., arrêt du 28 avril 2009, *K.H. et autres c. Slovaquie*, n° 32881/04, §§ 47-48 et 54.

585 *Ibidem*, § 56.

586 Cour eur. D.H., arrêt du 26 mai 2011, *R.R. c. Pologne*, n° 27.617/04, §§ 197-200.

587 Voy. Cour eur. D.H., arrêt du 10 février 2009, *Iordachi et autres c. Moldavie*, n° 25198/02, § 29 ; arrêt du 10 mars 2009, *Bykov c. Russie*, n° 4378/02 ; arrêt du 21 avril 2009, *Raducu c. Roumanie*, n° 70787/01, § 91 ; arrêt du 9 juin 2009, *Kvanisca c. Slovaquie*, n° 72094/01, § 76 ; arrêt du 18 mai 2010, *Kennedy c. Royaume-Uni*, n° 26839/05, § 118 ; arrêt du 24 mai 2011, *Association « 21 décembre 1989 » et autres c. Roumanie*, n° 33.810/07 et 18.817/08, § 167 ; décision du 7 septembre 2010, *Fernandez Saavedra & Reyes Cortes c. Espagne*, n° 47646/06, § 38.

suites pénales dirigées contre la personne concernée sont des ingérences d'une autorité publique dans l'exercice du droit au respect de la vie privée[588].

La crainte d'une surveillance secrète qui découle de l'existence même d'une législation prévoyant des mesures de surveillance non accompagnées de garanties suffisantes contre les ingérences arbitraires dans la vie privée et la correspondance des personnes est de nature à constituer une ingérence dans les droits reconnus par l'article 8[589].

Pour être acceptable, pareille ingérence doit être prévue par la loi, poursuivre un but légitime au regard de l'article 8.2 et être nécessaire dans une société démocratique afin de réaliser cet objectif. En ce qui concerne cette dernière condition, les États contractants jouissent d'une certaine marge d'appréciation pour juger de l'existence et de l'étendue de cette nécessité, mais elle va de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent, même quand elles émanent d'une juridiction indépendante. À cet effet, la Cour doit être convaincue de l'existence de garanties adéquates et suffisantes contre les abus[590].

Selon la jurisprudence constante de la Cour, la législation nationale doit fixer :

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

De plus, l'organe qui autorise une mesure de surveillance secrète doit être indépendant et il doit y avoir un contrôle judiciaire ou un contrôle par un autre organe indépendant de l'activité de cet organe[591].

L'utilisation d'enregistrements de communications téléphoniques auxquelles l'individu n'est pas partie dans le cadre de poursuites pénales dirigées contre lui, ne relève pas de l'article 8 mais bien de l'article 6 au titre de l'admissibilité des preuves[592].

L'interception d'une communication téléphonique du requérant réalisée par un particulier qui en transmet ensuite l'enregistrement au parquet ne constitue pas, en principe, une ingérence qui puisse être imputée aux autorités publiques, celles-ci ne pouvant pas être tenues responsables des actes des personnes privées (sous réserve, bien entendu, que ce particulier n'ait pas agi à l'ins-

588 Voy. Cour eur. D.H., arrêt du 21 avril 2009, *Raducu c. Roumanie*, n° 70787/01, § 91 ; arrêt du 9 juin 2009, *Kvanisca c. Slovaquie*, n° 72094/01, § 76 ; décision du 7 septembre 2010, *Fernandez Saavedra & Reyes Cortes c. Espagne*, n° 47646/06, § 38.

589 Cour eur. D.H., arrêt du 24 mai 2011, *Association « 21 décembre 1989 » et autres c. Roumanie*, n° 33.810/07 et 18.817/08, § 167.

590 Cour eur. D.H., décision du 7 septembre 2010, *Fernandez Saavedra & Reyes Cortes c. Espagne*, n° 47646/06, §§ 38 et 42-43.

591 Cour eur. D.H., arrêt du 10 février 2009, *Iordachi et autres c. Moldavie*, n° 25198/02, § 29. Voy. aussi : Cour eur. D.H., arrêt du 10 mars 2009, *Bykov c. Russie*, n° 4378/02.

592 Cour eur. D.H., arrêt du 30 juin 2009, *Viorel Borzo c. Roumanie*, n° 75109/01 et 12639/02, § 117.

tigation de ces mêmes autorités), d'autant plus que cet enregistrement n'a pas été utilisé à charge du requérant dans le cadre des poursuites pénales dirigées contre lui[593].

154. Surveillance vidéo. Dans la mesure où la notion de « vie privée » peut aussi s'étendre aux activités relevant de la sphère professionnelle ou commerciale et qu'il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée », la vie privée d'une personne peut être affectée par des mesures prises en dehors de son domicile ou de ses locaux privés. À cet égard, les attentes raisonnables de l'individu quant au respect de sa vie privée peuvent constituer un facteur important, quoique pas nécessairement décisif[594].

La surveillance des faits et gestes d'un individu dans un lieu public au moyen d'un dispositif de prise de vues ne mémorisant pas les données visuelles ne constitue pas en elle-même une forme d'ingérence dans la vie privée. En revanche, le fait de recueillir systématiquement de telles données et de les mémoriser peut soulever des questions liées à la vie privée. En ce sens, l'utilisation de caméras de surveillance sur les lieux du travail, dans des rues et dans des édifices publics, tels que des centres commerciaux ou des commissariats, où elles visent un but légitime et identifiable, ne soulève en elle-même aucune difficulté au regard de l'article 8.1[595].

Cependant, la surveillance secrète par des moyens techniques est une mesure exceptionnelle et constitue une ingérence grave dans le droit au respect de la vie privée et familiale garanti par l'article 8. Caractéristique de l'État policier, le pouvoir de surveiller en secret les citoyens n'est tolérable que dans la mesure strictement nécessaire à la sauvegarde des institutions étatiques, de la prééminence du droit, de la démocratie et des droits de l'homme.

Dans le cadre de poursuites pénales, les autorités internes ne doivent y recourir que lorsqu'il existe des éléments de preuve ou des indices convaincants de la préparation ou de la commission d'une infraction pénale. Par ailleurs, l'étendue et les limites dans le temps et dans l'espace de la surveillance secrète par des moyens techniques, ainsi que l'utilisation des données obtenues, doivent être strictement réglementées par la loi afin d'éviter tout abus. En outre, les individus faisant l'objet d'une telle mesure doivent pouvoir accéder aux images et informations obtenues par ces moyens techniques de surveillance, lesquelles ne doivent pas être utilisées en dehors de l'enquête en question. Ces individus doivent également disposer d'un recours devant les autorités judiciaires en cas d'utilisation abusive de la surveillance secrète[596].

Toujours dans le contexte de la surveillance secrète exercée par des autorités publiques, le droit interne doit offrir une protection contre l'ingérence arbitraire dans l'exercice du droit d'un individu au regard de l'article 8. En outre, la loi doit user de termes qui soient clairs pour indiquer aux individus de manière suffisante en quelles circonstances et sous quelles conditions elle habilite les autorités publiques à prendre pareilles mesures secrètes[597].

593 *Ibidem*, § 119.
594 Cour eur. D.H., décision du 11 janvier 2011, *Aydogdu et consorts c. Turquie*.
595 *Ibidem*.
596 *Ibidem*. La Cour se réfère à ce sujet à la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe.
597 Cour eur. D.H., décision du 11 janvier 2011, *Aydogdu et consorts c. Turquie*.

155. Surveillance par GPS (*Global Positioning System*). La Cour distingue la surveillance par GPS des surveillances visuelles ou acoustiques au motif que ces dernières sont, en règle générale, davantage susceptibles de porter atteinte au droit au respect de la vie privée car elles révèlent plus d'informations sur la conduite, les opinions ou les sentiments de l'individu qui en fait l'objet[598].

La surveillance par GPS ainsi que le traitement et l'utilisation des données obtenues grâce à celle-ci peuvent constituer une ingérence dans la vie privée de l'intéressé en tenant compte, notamment, des éléments suivants[599] :

- la durée de la surveillance ;
- l'objectif assigné à la collecte des informations sur l'individu ;
- la collecte et la conservation systématiques de données indiquant l'endroit où se trouvait l'individu et traçant ses déplacements en public ;
- l'enregistrement de données personnelles et leur utilisation pour suivre tous les déplacements de l'individu afin d'effectuer des investigations complémentaires et recueillir d'autres éléments de preuve dans les endroits où il s'est rendu, éléments ensuite utilisés dans le cadre de son procès pénal[600].

En principe, la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures de surveillance secrète. Eu égard au risque d'abus inhérent à tout système de surveillance secrète, de telles mesures doivent se fonder sur une loi particulièrement précise, en particulier compte tenu de ce que la technologie disponible devient de plus en plus sophistiquée[601].

Toutefois, ces principes relativement stricts édictés en matière d'écoutes téléphoniques ne sont pas applicables en tant que tels à la surveillance par GPS de déplacements en public. Tenant compte de ce qu'il s'agit d'une mesure de surveillance secrète par une autorité publique, de l'absence de contrôle public et du risque d'abus, la Cour doit être convaincue de l'existence de garanties adéquates et suffisantes contre les abus et les ingérences arbitraires dans l'exercice des droits garantis par l'article 8. Cette appréciation dépend de l'ensemble des circonstances de la cause, comme, par exemple, la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, et le type de recours fourni par le droit interne. À ce sujet, la Cour estime que l'existence d'un contrôle judiciaire ainsi que la possibilité d'exclure les éléments de preuve obtenus au moyen d'une surveillance illégale par GPS constituent déjà une garantie importante, en ce qu'elle décourage les autorités d'enquête de recueillir des preuves par des moyens illégaux. Dans le même

598 Cour eur. D.H., arrêt du 2 septembre 2010, *Uzun c. Allemagne*, n° 35623/05, § 52.

599 *Ibidem*.

600 *Ibidem*, §§ 50-51.

601 *Ibidem*, § 61. La Cour a ajouté que sous l'angle de l'article 7 de la Convention, aussi clair que le libellé d'une disposition légale puisse être, dans quelque système juridique que ce soit, y compris le droit pénal, il existe immanquablement un élément d'interprétation judiciaire. Il faut toujours élucider les points douteux et s'adapter aux changements de situation. D'ailleurs, il est solidement établi dans la tradition juridique des États parties à la Convention que la jurisprudence, en tant que source du droit, contribue nécessairement à l'évolution progressive du droit pénal. On ne saurait interpréter la Convention comme proscrivant la clarification graduelle des règles de la responsabilité pénale par l'interprétation judiciaire d'une affaire à l'autre, à condition que le résultat soit cohérent avec la substance de l'infraction et raisonnablement prévisible. La Cour estime que ces principes, développés sous l'angle de l'article 7, s'appliquent également au contexte examiné (*Id.*, § 62).

ordre d'idées, alors que les écoutes téléphoniques requièrent la délivrance d'un mandat par un organe indépendant, la Cour estime que le contrôle judiciaire ultérieur de la surveillance d'un individu par GPS offre une protection suffisante contre l'arbitraire[602].

Ceci étant, afin que les garanties contre les abus soient suffisantes lorsqu'un individu fait déjà l'objet d'autres mesures de surveillance, les mesures d'investigation prises par différentes autorités doivent être coordonnées et, avant d'ordonner, en plus, sa surveillance par GPS, le parquet doit s'assurer qu'il est au courant des autres mesures de surveillance préexistantes[603], ce qui renvoie à la question de l'admissibilité d'une surveillance totale de l'individu[604].

156. Surveillance des déplacements. La collecte et la conservation d'informations relatives aux déplacements en train ou en avion d'un individu dont le nom est repris dans une base de données de surveillance constituent une ingérence dans sa vie privée telle que protégée par l'article 8.1[605].

Ceci ne signifie pas que l'individu doit pouvoir prédire quand les autorités recourront à une surveillance secrète afin de pouvoir adapter son comportement à cette information. Toutefois, au vu des risques évidents d'arbitraire en particulier quand un pouvoir attribué au gouvernement s'exerce en secret, il est essentiel d'avoir des règles claires et détaillées sur l'application de mesures secrètes de surveillance, d'autant plus que les technologies disponibles sont de plus en plus sophistiquées. La loi doit être suffisamment claire dans son contenu afin de fournir aux citoyens des indications adéquates sur les conditions et circonstances dans lesquelles les autorités sont autorisées à recourir à des mesures de surveillance secrète et de collecte de données. De plus, en raison de l'absence de contrôle public et du risque d'abus intrinsèque à tout système de surveillance, les précautions minimales suivantes doivent être reprises dans une loi (formelle) afin d'éviter tout abus : la nature, l'étendue et les limites dans le temps des mesures possibles, les éléments requis pour les ordonner, les autorités compétentes pour les autoriser, les exécuter et les superviser, ainsi que le type de recours offerts par le droit national[606].

Ainsi, quand l'ordre ministériel qui gouverne la création et le fonctionnement de la base de données de surveillance n'est pas publié et n'est pas accessible au public, que les raisons pour lesquelles le nom d'une personne est repris dans la base de données, les autorités compétentes pour ordonner cet enregistrement, la durée de la mesure, la nature précise des données collectées, les procédures pour l'enregistrement et l'utilisation des données collectées, ainsi que les contrôles et garanties existantes contre les abus, ne sont pas ouverts au contrôle et à la connaissance du public, la législation nationale n'indique pas avec suffisamment de clarté l'étendue et les modalités de l'exercice du pouvoir discrétionnaire ainsi conférés aux autorités nationales de collecter et conserver des informations sur la vie privée des individus dans une base de données de surveillance. En particulier, il n'y a pas, comme l'exige pourtant la Cour dans sa jurisprudence

602 Cour eur. D.H., arrêt du 2 septembre 2010, *Uzun c. Allemagne*, n° 35623/05, §§ 63, 66 et 72.

603 La Cour n'indique pas le moment de cette information.

604 Cour eur. D.H., arrêt du 2 septembre 2010, *Uzun c. Allemagne*, n° 35623/05, § 73. À lire ce considérant, il pourrait en être déduit que la surveillance totale d'une personne ne serait, en principe, pas autorisée.

605 Cour eur. D.H., arrêt du 21 juin 2011, *Shimovolos c. Russie*, n° 30.194/09, § 66.

606 *Ibidem*, § 68.

(constante), d'indication sur les garanties minimales contre les abus qui soient énoncées sous une forme accessible au public[607].

157. Surveillance des employés. La vie privée d'un employé est concernée lorsque son comportement sur son lieu de travail fait l'objet d'un enregistrement vidéo à la demande de son employeur sans information préalable, que les images ainsi prises sont traitées et vues par plusieurs personnes qui travaillent pour l'employeur, et qu'ensuite, elles sont utilisées dans des procédures publiques devant les juridictions du travail.

La Cour examine, alors, si l'État a ménagé un juste équilibre entre le droit au respect de la vie privée de l'employé, l'intérêt de l'employeur à la protection de ses droits de propriété, et l'intérêt public à une bonne administration de la justice.

La Cour considère que la surveillance vidéo secrète sur le lieu de travail qui répond à de réels soupçons de vol ne concerne pas la vie privée dans une mesure comparable à celle induite par des atteintes graves à des aspects essentiels de la vie privée et pour lesquels la Cour a considéré qu'une protection législative était indispensable. C'est pourquoi la Cour a considéré, en tout cas dans l'affaire *Kopke c. Allemagne*[608], que la protection de la vie privée de l'employé, dans le contexte d'une surveillance vidéo secrète, pouvait être adéquatement protégée par la jurisprudence dégagée par les juridictions nationales en la matière sans que l'État ne soit obligé d'adopter un cadre législatif formel en exécution de son obligation positive découlant de l'article 8.

Ceci étant, la Cour a noté que la surveillance vidéo secrète d'un employé sur son lieu de travail devait être vue, en tant que telle, comme une ingérence importante dans sa vie privée, en ce qu'elle implique une documentation enregistrée et reproductible de son comportement sur son lieu de travail, et à laquelle l'employé, contraint d'exécuter son travail sur ce même lieu, ne pouvait pas se soustraire.

Toujours dans l'affaire *Kopke c. Allemagne*, la Cour a tenu compte des éléments suivants :
- il y avait des raisons matérielles de soupçonner le travailleur (disparition de stocks et irrégularités comptables) ;
- seule la personne soupçonnée faisait l'objet de la mesure de surveillance ;
- la surveillance était limitée dans le temps (deux semaines) et restreinte à un espace bien défini ;
- il s'agissait d'un lieu accessible au public ;
- les images n'ont été traitées que par un nombre limité de personnes (celles qui travaillaient pour l'agence de détectives et quelques membres du personnel de l'employeur) ;
- les images n'ont été utilisées que dans le cadre de la résolution du contrat de travail.

La Cour a, dès lors, considéré que l'ingérence avait été limitée à ce qui était nécessaire pour réaliser les finalités poursuivies par la vidéo surveillance, d'autant plus que l'employeur avait un intérêt considérable dans la protection de ses droits de propriété et qu'il devait pouvoir compter sur l'honnêteté de son employé en charge de la caisse. En ce sens, elle a considéré que l'intérêt de l'employeur à la protection de ses droits de propriété ne pouvait être effectivement sauve-

607 Cour eur. D.H., arrêt du 21 juin 2011, *Shimovolos c. Russie*, n° 30.194/09, §§ 69-70.
608 Cour eur. D.H., décision du 5 octobre 2010, *Kopke c. Allemagne*, n° 420/07.

gardé que s'il était autorisé à collecter des preuves du comportement infractionnel d'un employé afin de les utiliser devant les juridictions et s'il pouvait conserver les données collectées jusqu'au terme des procédures introduites par l'employé. La Cour a noté que ceci était également dans l'intérêt d'une bonne administration de la justice par les juridictions nationales qui devaient pouvoir établir la vérité autant que possible tout en respectant les droits des personnes concernées. De plus, elle a noté que la surveillance vidéo secrète avait permis d'innocenter les autres employés qui n'étaient coupables d'aucune infraction.

La Cour a, néanmoins, indiqué qu'il ne devait pas exister d'autre moyen moins attentatoire à la vie privée du travailleur qui eut permis de protéger de manière tout aussi efficace les droits de propriété de l'employeur. À cet égard, la Cour a considéré que ni l'inventaire des stocks ni la surveillance du travailleur par d'autres membres du personnel ni une vidéo surveillance « visible » n'auraient permis de mettre à jour les vols.

Ceci étant, la Cour a quand même ajouté que l'équilibre ici atteint par l'État entre les droits et intérêts en présence n'était pas la seule réponse au respect des obligations tirées de la Convention en la matière. Elle a aussi noté que les intérêts concurrents pourraient très bien recevoir un autre poids dans le futur, en tenant compte notamment de la mesure dans laquelle les intrusions dans la vie privée seraient réalisées grâce à de nouvelles, nombreuses et plus sophistiquées technologies[609].

158. Collecte, conservation et utilisation de données. La mémorisation dans un registre secret et la communication de données relatives à la « vie privée » d'un individu entrent dans le champ d'application de l'article 8.1. De même, des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics[610]. Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne[611].

La collecte systématique et la conservation de données sur des individus par des services de sécurité constituent une ingérence dans leur vie privée, même lorsque ces données sont collectées dans un lieu public ou qu'elles concernent exclusivement les activités professionnelles ou publiques de ces personnes[612].

Mais, si la mémorisation, par une autorité publique, de données relatives à la vie privée d'un individu peut constituer une ingérence au sens de l'article 8, peu importe que les informations mémorisées soient ou non utilisées par la suite, la Cour tient compte, afin de déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée, du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés[613].

609 Cour eur. D.H., décision du 5 octobre 2010, *Kopke c. Allemagne*, n° 420/07.

610 Cour eur. D.H., décision du 9 juin 2009, *RAD c. Roumanie*, n° 9742/04, § 34 ; arrêt du 17 février 2011, *Wasmuth c. Allemagne*, n° 12884/03, § 74 ; arrêt du 24 mai 2011, *Association « 21 décembre 1989 » et autres c. Roumanie*, n° 33.810/07 et 18.817/08, § 168.

611 Cour eur. D.H., décision du 9 juin 2009, *RAD c. Roumanie*, n° 9742/04, § 34.

612 Cour eur. D.H., arrêt du 21 juin 2011, *Shimovolos c. Russie*, n° 30.194/09, § 65.

613 Cour eur. D.H., arrêt du 18 octobre 2011, *Khelili c. Suisse*, n° 16.188/07, § 55.

Ainsi, dans l'affaire *Khelili c. Suisse*, la Cour a considéré que la mémorisation de données relatives à la vie privée de la requérante, dont faisait partie sa profession, ainsi que leur conservation, constituaient une ingérence au sens de l'article 8, car il s'agissait d'une donnée à caractère personnel se rapportant à un individu identifié ou identifiable. La Cour s'est alors référée aux principes dégagés dans l'affaire *S. et Marper c. Royaume-Uni* en matière de conservation d'informations à caractère personnel, ceux-ci reflétant les principes de base applicables aux traitements de données à caractère personnel (principe de finalité, de qualité et de durée de conservation des données, sans oublier leur sécurité). Dans ce cadre, la Cour a admis qu'il pouvait être conforme au principe de proportionnalité de conserver des données relatives à la vie privée d'une personne au motif que cette dernière pourrait récidiver. Toutefois, sans sous-estimer l'importance d'une prévention efficace de la criminalité, la Cour a considéré, eu égard, notamment, à l'importance primordiale de la présomption d'innocence dans une société démocratique, que le maintien de la mention « prostituée » comme profession de la requérante qui n'a jamais été condamnée pour exercice illicite de la prostitution ne répond pas à un « besoin social impérieux » au sens de l'article 8[614].

L'obligation faite à un individu d'indiquer sur sa carte d'imposition qu'il ne fait pas partie d'une église ou d'une société religieuse habilitées à prélever l'impôt cultuel et se prévalant de ce droit, constitue une ingérence dans son droit au respect de sa vie privée[615].

Dans des circonstances normales, seule la destruction ou la rectification des informations personnelles conservées par des autorités représente une solution effective à une violation de l'article 8[616].

159. Fichiers d'auteurs d'infractions sexuelles. En 2004, la France a créé un fichier judiciaire national automatisé des auteurs d'infractions sexuelles. C'est un fichier d'identification judiciaire à l'instar du fichier automatisé des empreintes digitales, du fichier national des empreintes génétiques et du casier judiciaire national[617].

La Cour a rappelé que la mémorisation par une autorité publique de données relatives à la vie privée d'une personne constituait une ingérence au sens de l'article 8, peu importe l'utilisation ultérieure des informations ainsi mémorisées[618]. L'obligation pour les personnes ayant fait l'objet d'une condamnation pour infraction sexuelle d'indiquer à la police leur nom, date de naissance, adresse ou changement d'adresse, relève de l'article 8.1[619], et l'obligation de justifier son adresse une fois par an et les changements d'adresse sous peine d'un emprisonnement et d'une amende n'est pas contraire aux principes de l'article 8[620].

614 *Id.*, §§ 56, 61-62, 66 et 68.

615 Cour eur. D.H., arrêt du 17 février 2011, *Wasmuth c. Allemagne*, n° 12884/03, § 74.

616 Cour eur. D.H., décision du 6 janvier 2011, *Kamburov c. Bulgarie*, n° 14.336/05, § 56. Ce ne sera donc pas toujours le cas, ce qui renvoie à la problématique des archives des anciens pays de l'Est comme la Bulgarie en l'espèce.

617 Cour eur. D.H., arrêt du 17 décembre 2009, *Bouchacourt c. France*, n° 5335/06, § 14 ; *M.B. c. France*, n° 22115/06, § 9 ; *Gardel c. France*, n° 16428/05, § 16.

618 Cour eur. D.H., arrêt du 17 décembre 2009, *Bouchacourt c. France*, n° 5335/06, § 57 ; *M.B. c. France*, n° 22115/06, § 49 ; *Gardel c. France*, n° 16428/05, § 58.

619 Cour eur. D.H., décision du 26 janvier 1999, n° 42293/98 ; arrêt du 17 décembre 2009, *Bouchacourt c. France*, n° 5335/06, § 57 ; *M.B. c. France*, n° 22115/06, § 49 ; *Gardel c. France*, n° 16428/05, § 58.

620 Cour eur. D.H., arrêt du 17 décembre 2009, *Bouchacourt c. France*, n° 5335/06, § 65 ; *M.B. c. France*, n° 22115/06, § 57 ; *Gardel c. France*, n° 16428/05, § 66.

L'existence d'une procédure judiciaire d'effacement des données dans le cadre du fichier judiciaire national automatisé des auteurs d'infractions sexuelles assure un contrôle indépendant de la justification de la conservation des informations sur la base de critère précis et présente des garanties suffisantes et adéquates du respect de la vie privée au regard de la gravité des infractions justifiant l'inscription sur le fichier. Certes, la mémorisation des données pour une période aussi longue que trente ans pourrait poser un problème sous l'angle de l'article 8, mais la Cour a noté que la personne pouvait, en tout état de cause, présenter une requête en effacement des données mémorisées alors que la décision ayant entraîné son inscription dans le fichier avait cessé de produire tous ses effets, et que, dans ces conditions, la durée de conservation des données n'était pas disproportionnée au regard du but poursuivi par la mémorisation des informations, étant la prévention et la répression de la récidive[621].

Par ailleurs, la Cour a constaté que si les modalités d'utilisation du fichier et le champ des autorités publiques qui ont accès audit fichier avaient été élargis et ne se limitaient plus aux autorités judiciaires et de police mais aussi à d'autres organes de l'administration, il n'en demeurait pas moins que la consultation de ces données était exclusivement accessible à des autorités astreintes à une obligation de confidentialité et dans des circonstances précisément déterminées[622].

160. Intégrité personnelle, droit à la réputation et à l'honneur. L'intégrité personnelle ne se confond pas avec la réputation. La réputation est traditionnellement protégée par des lois sur la diffamation comme portant originellement sur des intérêts financiers ou le statut social. Par contre, les droits relatifs à l'intégrité personnelle qui relèvent de l'article 8 ne concernent pas l'évaluation externe des personnes alors que cette évaluation est décisive en matière de réputation. Il est possible de perdre l'estime de la société sans perdre l'intégrité qui est inaliénable[623].

La Cour a précisé que, dans sa jurisprudence, la réputation n'avait été reconnue que sporadiquement en tant que droit indépendant et que lorsque cela avait été le cas, c'était au motif que les allégations présentaient une nature sérieusement offensante dont la publication avait un effet direct inévitable sur la vie privée de l'individu concerné. Si ce dernier ne démontre pas qu'une publication constitue une ingérence sérieuse avec sa vie privée en manière telle qu'elle porte atteinte à son intégrité personnelle, il ne reste, dès lors, en jeu que sa seule réputation dans le cadre d'une publication qui doit être conforme à l'article 10[624].

C'est dans cette mesure que l'article 8 englobe le droit à la protection de la réputation puisque la réputation d'une personne, même si celle-ci fait l'objet de critiques dans le contexte d'un débat public, fait partie de son identité personnelle et de son intégrité psychologique. La réputation relève, dès lors, également de sa vie privée, de la même façon que l'honneur[625]. Toutefois, pour que l'article 8 trouve à s'appliquer, l'attaque contre l'honneur personnel et la réputation doit atteindre un certain degré de gravité et, d'une certaine manière, causer un préjudice à la

621 Cour eur. D.H., arrêt du 17 décembre 2009, *Bouchacourt c. France*, n° 5335/06, § 68 ; *M.B. c. France*, n° 22115/06, § 60 ; *Gardel c. France*, n° 16428/05, § 69.

622 Cour eur. D.H., arrêt du 17 décembre 2009, *Bouchacourt c. France*, n° 5335/06, § 69 ; *M.B. c. France*, n° 22115/06, § 61 ; *Gardel c. France*, n° 16428/05, § 70.

623 Cour eur. D.H., arrêt du 28 avril 2009, *Karako c. Hongrie*, n° 39311/05, §§ 22-23.

624 Cour eur. D.H., arrêt du 28 avril 2009, *Karako c. Hongrie*, n° 39311/05, § 23.

625 Cour eur. D.H., arrêt du 9 avril 2009, *A. c. Norvège*, n° 28070/06, § 64 ; arrêt du 21 septembre 2010, *Polanco Torres & Movilla Polanco c. Espagne*, n° 34147/06, § 40.

jouissance personnelle du droit au respect de la vie privée[626]. Pour le dire autrement, les allégations factuelles doivent être suffisamment graves et leur publication doit avoir des répercussions directes sur la vie privée de la personne concernée. Pour que l'article 8 entre en jeu, la publication pouvant ternir la réputation d'une personne doit constituer une atteinte à sa vie privée d'une gravité telle que son intégrité personnelle en soit compromise[627].

Les États ont l'obligation positive de protéger le droit à la réputation des individus, en ce qu'il s'agit d'un élément de leur vie privée au sens de l'article 8[628]. Mais l'article 8 ne permet pas de se plaindre d'une atteinte à la réputation qui est la conséquence prévisible de son comportement comme, par exemple, la commission d'un acte criminel[629].

161. Protection de la vie privée et liberté d'expression. Dans les affaires où une violation des droits garantis par l'article 8 est alléguée et que l'ingérence invoquée avec ces droits trouve son origine dans une expression, quelle qu'en soit la forme, la Cour souligne que la protection fournie par l'État doit être entendue comme prenant en considération ses obligations sous l'article 10, cette dernière disposition ayant spécifiquement pour objet la liberté d'expression[630].

Toujours dans ces affaires, la Cour met en balance le droit au respect de la vie privée et l'intérêt public de la liberté d'expression, intérêt dans lequel les journalistes ont un rôle clé en qualité de « chien de garde ». Ce faisant, la Cour souligne qu'il n'existe pas de hiérarchie entre les droits garantis par ces deux dispositions de la Convention[631].

La Cour tient compte de la contribution des photographies et articles publiés dans la presse à un débat d'intérêt général[632].

La Cour insiste, par ailleurs, sur le rôle prééminent de la presse dans l'information du public et dans la diffusion d'informations et d'idées dans des matières d'intérêt public, dans un État de droit. Non seulement la presse a la tâche de diffuser ces informations et idées mais le public a aussi le droit de les recevoir. Autrement, la presse ne serait pas en mesure de jouer son rôle vital de « chien de garde »[633].

Ainsi, pour savoir si un État a atteint un juste équilibre entre le droit au respect de la vie privée d'un individu et la liberté d'expression du journal, la Cour prend en compte l'obligation positive de l'État tirée de l'article 8 de protéger la vie privée d'individus visés dans des procédures pénales en cours, ainsi que la liberté de la presse de communiquer des informations sur un sujet d'intérêt

626 Cour eur. D.H., arrêt du 9 avril 2009, *A. c. Norvège*, n° 28070/06, § 64.

627 Cour eur. D.H., arrêt du 21 septembre 2010, *Polanco Torres & Movilla Polanco c. Espagne*, n° 34147/06, § 40.

628 Pour un cas d'atteinte à la réputation par un rapport de police affirmant la culpabilité d'une personne en l'absence de poursuite pénale à son encontre, voy. : Cour eur. D.H., arrêt du 18 janvier 2011, *Mikolajova c. Slovaquie*, n° 4.479/03, § 53.

629 *Id.*, § 57.

630 Cour eur. D.H., arrêt du 28 avril 2009, *Karako c. Hongrie*, n° 39311/05, § 20 ; arrêt du 12 octobre 2010, *Timciuc c. Roumanie*, n° 28.999/03, § 144.

631 Cour eur. D.H., arrêt du 12 octobre 2010, *Timciuc c. Roumanie*, n° 28.999/03, § 144.

632 *Id.*, § 145.

633 Cour eur. D.H., arrêt du 10 mai 2011, *Mosley c. Royaume-Uni*, n° 48009/08, § 112.

public en ce compris les procédures pénales en cours, et le droit du public de recevoir cette information[634].

Dans l'affaire *A. c. Norvège*, la Cour a jugé que l'État devait se voir reconnaître une large marge d'appréciation dans l'évaluation du besoin de protéger la vie privée du requérant par rapport à la sauvegarde de la liberté d'expression du journal[635].

C'est dans le cas de débats ou de questions d'intérêt public général que l'étendue de la critique acceptable est plus grande envers des politiciens ou toutes autres figures publiques que pour des particuliers, dès lors que les premiers, au contraire des seconds, se sont exposés volontairement à un contrôle plus attentif de leurs faits et gestes tant par les journalistes que par le public en général et qu'ils doivent, dès lors, montrer une plus grande tolérance[636].

La Cour a rappelé la distinction entre la constatation de faits et les jugements de valeurs, soulignant que si l'existence de faits pouvait être démontrée, les jugements de valeur n'étaient pas susceptibles de preuve. Dès lors, l'exigence de prouver la véracité d'un jugement de valeur était impossible à rencontrer et violait la liberté d'expression. La Cour a précisé que la distinction entre la constatation d'un fait et le jugement de valeur relevait de la marge d'appréciation des autorités nationales et, en particulier, des juridictions nationales. Cependant, même en présence d'un jugement de valeur, il doit exister une base factuelle suffisante pour le fonder, sinon il serait excessif[637].

La Cour a aussi distingué la constatation de faits, même controversés, susceptibles de contribuer à un débat d'intérêt public général dans une société démocratique, par rapport à des allégations sordides sur la vie privée d'un individu. En ce qui concerne les premiers, le rôle prééminent de la presse dans une démocratie et sa tâche d'agir en tant que « chien de garde » sont des considérations importantes en faveur d'une conception restrictive à toute limite à la liberté d'expression. Par contre, la presse à sensation qui vise à satisfaire la curiosité d'un certain lectorat sur les aspects de la vie privée de certaines personnes ne mérite pas la même protection que celle conférée par l'article 10 à la presse. En conséquence, dans ce type d'affaires, la liberté d'expression appelle une interprétation plus étroite[638].

Ceci étant, la liberté journalistique comprend aussi la possibilité de recourir à un certain degré d'exagération, voire de provocation[639].

Dans l'affaire *Palade c. Roumanie*, le requérant se plaignait d'avoir été surnommé « Gogu le Boucher » après avoir tué plusieurs personnes, les avoir découpées en morceaux et éparpillé ces derniers dans des poubelles de la ville. La Cour a rappelé que le droit au respect de la vie privée du requérant devait être mis en balance avec l'intérêt public de la liberté d'expression, intérêt dans lequel les journalistes ont un rôle clé en qualité de « chien de garde »[640].

634 Cour eur. D.H., arrêt du 9 avril 2009, *A. c. Norvège*, n° 28070/06, § 65. Voy. aussi Cour eur. D.H., arrêt du 21 septembre 2010, *Polanco Torres & Movilla Polanco c. Espagne*, n° 34147/06, § 41.

635 Cour eur. D.H., arrêt du 9 avril 2009, *A. c. Norvège*, n° 28070/06, § 66.

636 Cour eur. D.H., arrêt du 30 mars 2010, *Petrenco c. Moldavie*, n° 20928/05, § 55. Voy. aussi Cour eur. D.H., arrêt du 12 octobre 2010, *Timciuc c. Roumanie*, n° 28.999/03, § 150.

637 Cour eur. D.H., arrêt du 30 mars 2010, *Petrenco c. Moldavie*, n° 20928/05, § 56.

638 Cour eur. D.H., arrêt du 10 mai 2011, *Mosley c. Royaume-Uni*, n° 48009/08, § 114.

639 Cour eur. D.H., décision du 31 août 2010, *Palade c. Roumanie*, n° 37441/05, § 28.

640 *Id.*, § 27.

Elle a aussi indiqué que si les juridictions judiciaires étaient bien les lieux de détermination de la culpabilité ou de l'innocence d'un individu poursuivi pénalement, cela ne signifiait pas qu'il ne pouvait pas y avoir de débat préalable ou contemporain à ce sujet dans d'autres lieux, que ce soit dans des journaux spécialisés, dans la presse en général ou dans le public. Toutefois, les commentaires admissibles sur des procédures pénales en cours ne peuvent pas s'étendre à ceux qui sont susceptibles de porter préjudice, que ce soit intentionnellement ou non, aux chances d'un individu à un procès équitable, ou qui sont de nature à porter atteinte à la confiance du public dans le rôle des juridictions judiciaires dans l'administration de la justice[641].

La diffusion d'images des ébats sexuels du président de la fédération internationale de l'automobile a donné l'occasion à la Cour de rappeler que la publication d'articles, de photographies et d'images vidéo d'un individu participant à des actes sexuels avait un impact significatif sur son droit au respect de la vie privée[642].

Comme les médias audiovisuels ont un effet plus immédiat et plus puissant que les médias imprimés et bien que la liberté d'expression comprenne aussi la publication de photographies, la Cour a rappelé que, dans ce cas, la protection des droits d'autrui revêt une importance particulière, notamment quand les images contiennent des informations très personnelles et très intimes d'un individu ou quand elles ont été prises dans un lieu privé et clandestinement en recourant à des équipements d'enregistrements secrets. Les éléments pertinents à prendre en compte pour apprécier l'équilibre entre les intérêts concurrents résident dans la contribution complémentaire que pourrait apporter la publication de ces photographies à un débat d'intérêt général, ainsi que le contenu de ces photographies[643].

162. Notification préalable d'une publication par la presse. La Cour a considéré que si l'article 10 n'empêchait pas d'imposer des contraintes préalables à une publication, les dangers y afférents étaient tels qu'elles appelaient un contrôle des plus stricts. C'est d'autant plus le cas en ce qui concerne la presse que la durée de vie des nouvelles est très brève et que tout retard à leur publication, même pour une courte période, peut leur enlever toute valeur et intérêt. Toutefois, la Cour a admis que des contraintes préalables pourraient être plus facilement acceptables s'il était démontré qu'il n'y avait pas de nécessité pour une publication immédiate qui n'apportait pas de contribution évidente à un débat d'intérêt public général[644].

Au vu de l'effet inhibiteur que pourrait avoir une exigence de notification préalable d'une publication, ainsi qu'aux doutes importants quant à l'effectivité de pareille mesure et à la large marge d'appréciation de l'État en la matière, la Cour a jugé que, dans ces conditions, l'article 8 ne requérait pas l'imposition par la loi d'une mesure de notification préalable d'une publication[645].

163. Protection de la réputation et liberté d'expression. Dans le contexte des obligations positives découlant de l'article 8, l'État doit ménager un juste équilibre entre le droit du requérant à la protection de sa réputation, élément du droit à la protection de la vie privée, et le droit de

641 Cour eur. D.H., décision du 31 août 2010, *Palade c. Roumanie*, n° 37441/05, § 27. Voy. aussi Cour eur. D.H., arrêt du 12 octobre 2010, *Timciuc c. Roumanie*, n° 28.999/03, § 146.

642 Cour eur. D.H., arrêt du 10 mai 2011, *Mosley c. Royaume-Uni*, n° 48009/08, § 71.

643 *Id.*, § 115.

644 *Id.*, § 117.

645 *Id.*, § 132.

la partie adverse à la liberté d'expression protégée par l'article 10, étant entendu que la liberté d'expression peut être soumise à certaines restrictions proportionnées en vue de protéger la réputation d'autrui[646].

La Cour a rappelé le rôle essentiel de la presse dans une société démocratique. Ainsi, si la presse ne doit pas franchir certaines limites, s'agissant notamment de la protection de la réputation et des droits d'autrui, il lui incombe, néanmoins, de communiquer, dans le respect de ses devoirs et responsabilités, des informations et des idées sur toutes les questions d'intérêt général, en ce compris celles qui concernent le fonctionnement du pouvoir judiciaire[647].

En même temps, il y a lieu de rappeler que la garantie offerte par l'article 10 aux journalistes, en ce qui concerne les comptes rendus sur des questions d'intérêt général, est subordonnée à la condition que les intéressés agissent de bonne foi sur la base de faits exacts et fournissent des informations « fiables et précises » dans le respect de la déontologie journalistique, dont le contrôle revêt une importance accrue. Ainsi, il doit exister des motifs spécifiques pour relever les médias de leur obligation de vérifier des déclarations factuelles diffamatoires à l'encontre de particuliers. À cet égard, la nature et le degré de la diffamation en cause doivent être pris en compte ainsi que la question de savoir à quel point le média peut raisonnablement considérer que ses sources sont suffisamment crédibles. Cette dernière question doit s'envisager sous l'angle de la situation telle qu'elle se présentait au journaliste à l'époque et non avec le recul[648].

164. Divulgation de la séropositivité. Lorsqu'un individu se prévalant d'une incapacité permanente absolue de travail réclame en justice le paiement d'une indemnisation à ce titre à sa compagnie d'assurances, l'injonction judiciaire ordonnant le dépôt de son dossier médical au dossier de la procédure est nécessaire pour assurer le bon déroulement de la procédure[649].

165. L'indication de l'identité d'un individu. L'indication de l'identité d'un individu en toutes lettres dans des décisions judiciaires en rapport avec son état de santé constitue une « ingérence de l'autorité publique » dans l'exercice du droit au respect de la vie privée lorsque l'individu a expressément demandé que son identité demeure confidentielle. Compte tenu de la nécessité de protéger les informations relatives à la séropositivité, cette ingérence n'est pas justifiée lorsqu'elle ne se fonde pas sur des motifs impérieux, surtout lorsque la pratique nationale permet d'omettre l'identification de certaines parties à un procès notamment lorsque la protection de la vie privée de l'un ou l'autre le requiert[650].

166. Protection de la correspondance des détenus. La seule ouverture de la correspondance d'un détenu s'analyse en une ingérence dans l'exercice du droit au respect de la vie privée[651] et

646 Cour eur. D.H., arrêt du 21 septembre 2010, *Polanco Torres & Movilla Polanco c. Espagne*, n° 34147/06, § 41. Sur un cas relatif à la protection de la réputation dans le cadre d'un communiqué de presse de la direction d'une télévision publique donnant une version des faits portant sur le licenciement d'une réalisatrice d'émissions, voy. Cour eur. D.H., arrêt du 3 mai 2011, *Sipos c. Roumanie,* n° 26125/04.

647 Cour eur. D.H., arrêt du 21 septembre 2010, *Polanco Torres & Movilla Polanco c. Espagne*, n° 34147/06, § 42. Voy. aussi Cour eur. D.H., arrêt du 10 mai 2011, *Mosley c. Royaume-Uni*, n° 48009/08, § 113.

648 Cour eur. D.H., arrêt du 21 septembre 2010, *Polanco Torres & Movilla Polanco c. Espagne*, n° 34147/06, § 43.

649 Cour eur. D.H., 6 octobre 2009, *C.C. c. Espagne*, n° 1425/06, § 29.

650 *Id.*, §§ 26, 30 et s.

651 Cour eur. D.H., arrêt du 10 décembre 2009, *Mikhaylyuk et Petrov c. Ukraine*, n° 11932/02, § 24.

le contrôle de la correspondance médicale d'un détenu par l'officier médecin de la prison doit répondre à un juste équilibre avec le droit au respect de sa vie privée[652].

167. Accès à des services de santé. La Convention ne garantit pas en tant que tel le droit à des soins médicaux gratuits ou à des services de santé spécifiques. Par contre, l'article 8 trouve à s'appliquer à des situations où il n'y a pas assez de services médicaux disponibles[653].

168. Tests génétiques post-mortem. La conservation ou la destruction de prélèvements effectués sur un cadavre à des fins d'expertise et notamment d'identification génétique ne constitue pas une ingérence dans les droits garantis par l'article 8[654].

169. Examen psychiatrique forcé. Un examen forcé par un psychiatre d'un établissement public et le diagnostic qui s'en est suivi constituent une ingérence dans la vie privée de l'individu concerné[655].

B. La liberté d'expression et les nouvelles technologies

Quentin Van Enis[656]

170. Introduction. Durant les trois années couvertes par la présente chronique (2009-2011), la liberté d'expression a connu d'importants développements jurisprudentiels sur le terrain des nouvelles technologies. Au cours de la période examinée, la Cour européenne des droits de l'homme a rendu ses premiers arrêts concernant la liberté de parole sur le réseau des réseaux. En Belgique, les juges ont dû plus d'une fois s'employer à combler les lacunes d'un droit des médias désuet et souvent inadapté aux nouveaux moyens de communication. On songe en particulier au régime constitutionnel de la presse, pensé dans le contexte de l'imprimé, et que la Cour de cassation a (enfin) entrepris de dépoussiérer en admettant que des « délits de presse » peuvent être commis par le biais d'écrits numériques. Pour la clarté du propos, et dans la continuité de la précédente chronique (2002-2008), les décisions qui touchent au commerce électronique seront examinées ailleurs.

1. Le principe et la portée de la liberté d'expression sur l'internet

a. Le principe de la liberté d'expression sur l'internet

171. L'article 10 de la Convention européenne. À l'occasion de l'affaire *Times Newspapers Limited contre Royaume-Uni,* la Cour européenne des droits de l'homme a rendu son premier arrêt reconnaissant l'applicabilité de la garantie de l'article 10 aux propos exprimés sur l'internet. La Cour a ainsi mis fin à un suspense tout relatif en affirmant que « grâce à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites Internet contri-

652 Voy. à ce sujet : Cour eur. D.H., arrêt du 2 juin 2009, *Szuluk c. Royaume-Uni*, n° 36936/05, § 54.
653 Cour eur. D.H., arrêt du 26 mai 2011, *R.R. c. Pologne*, n° 27.617/04, § 198.
654 Cour eur. D.H., arrêt du 30 juin 2011, *Girard c. France*, n° 22.590/04, § 107 avec renvoi au § 99.
655 Cour eur. D.H., arrêt du 7 juillet 2011, *Fyodorov & Fyodorova c. Ukraine*, n° 39.229/03, § 82.
656 Assistant et doctorant à l'Université de Namur.

buent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information »[657].

b. L'application de l'interdiction des mesures préventives aux propos diffusés sur l'internet

172. L'article 19 de la Constitution. Si la portée de l'interdiction de la censure (article 25, alinéa 1er de la Constitution) reste controversée[658], il découle de l'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *RTBF contre Belgique* que l'article 19 de la Constitution doit être lu comme prohibant de manière générale les mesures préventives, et donc également s'agissant des médias autres que la presse écrite imprimée[659].

173. Le critère de la diffusion préexistante. Jugé qu'il n'y a pas lieu d'interdire préventivement la diffusion d'un article sur le net dès lors que « les requérants ne rapportent pas la preuve de ce que ''l'article litigieux est d'ores et déjà reproduit et commenté sur internet'' et parce que la mesure sollicitée apparaît comme une ingérence disproportionnée dans la liberté d'expression dans une société démocratique en ce sens qu'elle ne répond pas à un besoin social impérieux »[660]. Sans se prononcer sur la portée de l'article 25 de la Constitution, le juge a ainsi transposé à l'univers numérique le critère de la diffusion préexistante dégagé par la Cour de cassation en matière de presse écrite[661] et entériné par la Cour européenne des droits de l'homme[662] pour délimiter le champ d'application temporel de l'interdiction des mesures préventives.

174. L'absence d'obligation d'informer la personne concernée par une publication future. Dans l'affaire *Mosley contre Royaume-Uni*, la Cour européenne des droits de l'homme a jugé que n'enfreignait pas l'article 8 de la Convention (droit au respect de la vie privée) l'inexistence en droit anglais d'une obligation pour les médias d'avertir la personne visée par un reportage de leur intention de le publier, aux fins de permettre à cette dernière d'agir en référé pour en faire interdire la diffusion[663]. En l'espèce, le requérant n'avait pas réussi à faire cesser la dissémination sur l'internet d'une vidéo dépeignant des épisodes de sa vie sexuelle, même si des dommages et intérêts lui avaient été octroyés. L'arrêt regorge d'enseignements intéressants sur les rapports entre la liberté d'expression et la protection de la vie privée. Bornons-nous à signaler ici que la Cour y admet que l'existence d'un mécanisme de responsabilité *a posteriori* sanctionnant les abus de la liberté d'expression suffit à satisfaire aux exigences conventionnelles dérivant du droit au respect de la vie privée[664]. Cela étant, la Cour rappelle qu'à lui seul, l'article 10 n'interdit pas toute forme d'ingérence préventive dans la liberté d'expression même si de telles mesures appellent

657 Cour eur. D.H. (4e sect.), 10 mars 2009, arrêt *Times Newspapers Limited (nos 1 et 2) contre Royaume-Uni*, § 27, *R.D.T.I.*, 2009, p. 87, obs. Q. Van Enis.

658 Sur cette controverse, voy. notamment J. Englebert, « Le statut de la presse : du ''droit de la presse'' au ''droit de l'information'' », *Rev. dr. ULB*, 2007/35, pp. 229-288, spéc. pp. 266-274, nos 35-45.

659 Cour eur. D.H. (2e sect.), 29 mars 2011, arrêt *RTBF contre Belgique*, § 108, *J.L.M.B.*, 2011, p. 1244, obs. Q. Van Enis ; *J.T.*, 2012, p. 238, obs. K. Lemmens.

660 Civ. Bruxelles (prés.), 6 novembre 2009, *A&M*, 2010, p. 303.

661 Cass. (1re ch.), 29 juin 2000, *Pas.*, I, 2000, no 420.

662 Cour eur. D.H., 9 novembre 2006, arrêt *Leempoel & S.A. ED. Ciné Revue contre Belgique*, §§ 57 et 87, *J.L.M.B.*, 2007, p. 292, obs. P. Lambert ; *J.T.*, 2006, p. 789, obs. N. Bonbled et M. Lys.

663 Cour eur. D.H. (4e sect.), 10 mai 2011, arrêt *Mosley contre Royaume-Uni*, § 132.

664 *Ibid.*, § 120.

de sa part un contrôle particulièrement strict[665]. Au passage, la haute juridiction européenne observe que des restrictions préalables pourraient plus facilement être admises lorsqu'aucune urgence à publier n'est démontrée et qu'il n'y a pas de contribution manifeste à un débat d'intérêt général[666].

175. La proportionnalité de la suppression de contenus de sites d'informations. Fût-il prononcé après une première diffusion, le retrait pur et simple d'informations de l'internet est apparu suspect aux yeux de plusieurs juges.

Ainsi, la suppression d'un article d'un journal syndical ainsi que sa désindexation du moteur de recherche *Google*, au motif qu'il contenait les noms d'anciens actionnaires d'une société tombée en faillite, ont été jugées disproportionnées et partant ont été refusées par le tribunal de première instance d'Hasselt[667]. Les juges ont justifié leur décision en s'appuyant sur l'écoulement du temps (4 ans) entre la publication de l'article et la demande de retrait. Pareille motivation ne laisse pas de surprendre[668], compte tenu de la jurisprudence de la Cour européenne qui laisse aux États une plus grande marge de manœuvre s'agissant d'informations qui ont trait à des événements passés[669].

Dans une autre affaire, la cour d'appel d'Anvers a également refusé d'ordonner le retrait de la toile de l'intégralité d'un article publié par une association active dans l'analyse critique des méthodes thérapeutiques alternatives et qui avait taxé un médecin de « charlatan savant ». Les juges anversois ont toutefois accepté d'enjoindre à l'association défenderesse d'en supprimer certains passages diffamatoires[670].

En revanche, dans le domaine des pratiques de marché, la cessation de la diffusion de propos dénigrants a été jugée conforme au principe de la liberté d'expression. Ainsi, au terme d'un raisonnement assez sommaire, le président du tribunal de commerce d'Audenarde a fait droit à la demande d'une entreprise de faire cesser la diffusion sur l'internet d'un article peu flatteur émanant d'une société concurrente[671]. De la même manière, la cour d'appel de Bruxelles a ordonné la cessation du comportement d'un commerçant gestionnaire d'un site de petites annonces sur Internet qui, sur un forum de discussion, avait accusé une société spécialisée dans le référencement d'user de pratiques déloyales[672].

665 *Ibid.*, § 117.

666 *Ibid.*, § 117.

667 Civ. Hasselt (4e ch. A), 14 juin 2010, *A&M*, p. 250, note D. Voorhoof. Pour un autre exemple de refus, voy. Civ. Anvers (prés.), 24 novembre 2010, *A&M*, 2011, p. 565, note D. Voorhoof.

668 Voy. aussi la note critique de D. Voorhoof, « Kritiek in vakbondsmagazine mag robuust zijn, maar zonder naamsvermelding van de geviseerde aandeelhouders », *A&M*, 2011, p. 259.

669 Cour eur. D.H. (4e sect.), 10 mars 2009, arrêt *Times Newspapers Limited (nos 1 et 2) contre Royaume-Uni*, précité, § 45. Voy. *infra*, nos développements sur la prescription du délit de presse en ligne.

670 Anvers (2e ch.), 23 juin 2010, *A&M*, 2011, p. 223, note D.V. ; *NjW*, 2010, 790, note E.B. L'arrêt a été censuré sur ce point par la Cour de cassation, au motif qu'il ne résultait pas de la décision du juge du fond que le contexte d'expression de l'opinion avait bien été pris en compte avant d'imposer une restriction à la liberté d'expression. Voy. Cass. (1re ch.), 12 janvier 2012, *A&M*, 2012, p. 358, note D. Voorhoof.

671 Comm. Audenarde, 10 mars 2011, *A&M*, 2012, p. 383, note critique D. Voorhoof.

672 Bruxelles (9e ch.), 9 juillet 2010, *J.L.M.B.*, p. 1576.

c. La place de l'internet dans le paysage médiatique

176. L'interdiction d'apposer dans l'espace public une affiche renvoyant vers un site Internet. La prohibition de l'affichage dans l'espace public d'une publicité comportant l'adresse d'un site Internet licite d'une association dont certains membres sont accusés de sévices sexuels envers des mineurs, militant pour l'établissement d'une « géniocratie » et offrant des services de clonage, a été jugée proportionnée à l'objectif de la protection de la santé et de la morale et à la prévention du crime par une majorité de juges dans l'affaire *Mouvement raëlien suisse contre Suisse*[673]. À travers l'opposition entre majorité et minorité de la chambre saisie, l'affaire laisse apparaître l'ambivalence de la place de l'internet dans le paysage médiatique. Le Web doit-il jouer le rôle de valve de sécurité en contribuant à la proportionnalité des interdictions de diffusion touchant les autres médias[674] ou doit-on considérer, par un impératif de cohérence, que la diffusion licite d'un propos sur l'internet justifie l'admissibilité de sa dissémination par le biais d'autres médias (tel, en l'occurrence, l'affichage dans l'espace public)[675] ?

2. La mise en œuvre de la responsabilité en cas d'abus de la liberté d'expression sur le net

a. La compétence de la cour d'assises en matière de « délits de presse »

177. Introduction. Aux termes de l'article 150 de la Constitution, les « délits de presse » ressortissent à la compétence exclusive de la cour d'assises[676]. Une exception a toutefois été instaurée en 1999 s'agissant des délits de presse inspirés par le racisme ou la xénophobie[677].

178. L'application à l'internet. Si nombreux sont les juges qui, dans la période examinée, ont admis que des propos diffusés sur la toile peuvent constituer un délit de presse[678] de nature à entraîner l'application de l'article 150 et de la compétence du jury populaire – mieux nommée impunité pénale de fait, compte tenu de la politique de non-poursuite de la part des parquets généraux[679] –, ce sont surtout deux récents arrêts de la Cour de cassation qui retiennent l'attention.

673 L'arrêt a été confirmé, à une courte majorité, par la grande chambre de la Cour, laquelle a rendu son arrêt le 13 juillet 2012.

674 Voy. en particulier le § 58 de l'arrêt : « En ce qui concerne la proportionnalité de la mesure litigieuse, la Cour observe que cette dernière est strictement limitée à l'affichage sur le domaine public. Selon le Tribunal fédéral, la requérante demeure libre d'exprimer ses convictions par les nombreux autres moyens de communication à sa disposition (…) Il n'a notamment jamais été question d'interdire l'association requérante en tant que telle ni son site internet ».

675 Voy., en ce sens, l'opinion dissidente des juges Rozakis et Vajic qui soulignent notamment que : « De nos jours, vu la place et le rôle que jouent les communications directes telles que les téléphones portables et Internet, il paraît difficile à comprendre qu'une association légale disposant de son site Internet non interdit ne puisse pas utiliser les espaces publics pour promouvoir les mêmes idées par des affiches qui ne sont pas illicites et ne choquent pas le public ».

676 Il a tôt été admis que cette compétence exclusive ne concerne que l'action publique et laisse intactes les règles de l'action civile (Cass. (1re ch.), 24 janvier 1863, *Pas.*, 1864, p. 110).

677 Voy. récemment B. Renauld, *La lutte contre le racisme*, Waterloo, Kluwer, 2011, spéc. pp. 102-104.

678 Voy. p. ex. Civ. Bruxelles (75e ch.), 15 octobre 2009, *J.T.*, 2010, p. 254, *J.L.M.B.*, 2010, p. 128, note C. Dony (vidéo postée sur le site *YouTube*) ; *A&M*, 2010, p. 119 ; Bruxelles (11e ch.), 17 mars 2010, *J.T.*, 2010, p. 506, note Q. Van Enis ; *A&M*, 2010, p. 297, note S. Carneroli (message posté sur un forum de discussion) ; Gand (6e ch.), 28 mars 2011, no C/555/11, inédit ; Gand (4e ch.), 14 juin 2011, *A&M*, 2012, p. 251.

679 Dernièrement, un délit de presse a cependant été renvoyé devant la cour d'assises par la chambre des mises en accusation de Bruxelles. Voy. J. Englebert, « Vers un retour du délit de presse en cour d'assises ? », *A&M*, 2012, p. 102.

En effet, alors qu'on aurait pu penser qu'elle maintiendrait son exigence de l'écrit imprimé[680] pour refuser le qualificatif de « délit de presse » aux opinions abusivement diffusées sur le net, la Cour de cassation a opté pour une interprétation évolutive de la « presse », à tout le moins s'agissant d'écrits[681]. Les deux arrêts comportent un passage commun : le moyen qui fait valoir que « la propagation et la diffusion d'une opinion punissable ne peuvent constituer un délit de presse que par voie de presse écrite[682], manque en droit ». Le second arrêt rappelle, quant à lui, que « le délit de presse exige l'expression délictueuse d'une opinion dans un texte reproduit au moyen de la presse ou d'un procédé similaire » et admet que pareille exigence est remplie dès lors que « la distribution numérique constitue un tel procédé similaire ».

b. La prescription du « délit de presse » en ligne

179. L'archivage des informations sur l'internet. Le principal enjeu de l'affaire *Times Newspapers*, portée devant la Cour de Strasbourg, résidait dans la question de la prescription du délit de presse en ligne[683]. À cet égard, le droit anglais considère chaque consultation d'un article litigieux comme constitutive d'un nouvel acte de publication, entraînant un nouveau départ pour le délai de prescription, qui se révèle ainsi potentiellement infini (« *Internet publication rule* »).

De manière générale, dans son arrêt, la Cour européenne a reconnu aux États « une latitude plus large pour établir un équilibre entre les intérêts concurrents lorsque les informations sont archivées et portent sur des événements passés que lorsqu'elles ont pour objet des événements actuels »[684]. En l'espèce, la Cour n'a pas jugé nécessaire de se prononcer sur l'admissibilité dudit régime de prescription[685]. En effet, les juges de Strasbourg ont relevé que la société requérante, éditrice du journal, assurait elle-même la gestion de son service d'archives et que, pour échapper à toute responsabilité, elle n'était pas tenue de retirer les articles du site Internet, mais aurait pu se contenter d'y faire figurer un avertissement succinct reconnaissant leur caractère diffamatoire ou potentiellement diffamatoire, ce qu'elle n'avait fait que tardivement[686]. Au demeurant, la Cour n'a aperçu aucune raison de penser que le passage du temps ait compromis la défense de la société requérante étant donné que cette dernière avait déjà fait l'objet d'une action en diffamation, rapidement intentée, à raison des mêmes articles publiés dans la version papier du journal[687].

680 Voy. not. Cass. (1re ch.), 2 juin 2006, *J.L.M.B.*, 2006, p. 1402, obs. F. Jongen.

681 Cass. (2e ch.), 6 mars 2012, P.11.0855 : « Het middel dat ervan uitgaat dat enkel vermenigvuldiging en verspreiding van een strafbare meningsuiting door gedrukte geschriften een drukpersmisdrijf kan opleveren, faalt naar recht » (*J.L.M.B.*, 2012, p. 790 ; *J.T.*, 2012, p. 505, obs. Q. Van Enis ; *NjW*, 2012, p. 342, note E.B., *A.P.T.*, 2012, p. 491) et Cass. (2e ch.), 6 mars 2012, P.11.1374 : « Het drukpersmisdrijf vereist een strafbare meningsuiting in een tekst die vermenigvuldigd is door een drukpers of een gelijkaardig procedé. Digitale verspreiding vormt een dergelijk gelijkaardig procedé. Het onderdeel dat ervan uitgaat dat enkel vermenigvuldiging en verspreiding van een strafbare meningsuiting door een drukpers een drukpersmisdrijf kan opleveren, faalt naar recht » (*A&M*, 2012, p. 253, note D. Voorhoof ; *NjW*, 2012, p. 341, note E.B. ; *A.P.T.*, 2012, p. 491 ; *R.A.B.G.*, 2012, p. 877, et concl. av. gén. M. De Swaef ; *N. C.*, 2012, p. 223, et concl. av. gén. M. De Swaef).

682 Dans leur version originale, les deux arrêts utilisaient respectivement les expressions néerlandaises « door *gedrukte* geschriften » et « door een *druk*pers » (nous soulignons) qui emportent une connotation d'imprimé dont les mots français « par voie de presse écrite » ne rendent pas compte.

683 Arrêt précité.

684 *Ibid.*, § 45.

685 *Ibid.*, § 48.

686 *Ibid.*, § 47.

687 *Ibid.*, § 48.

En Belgique, dans une affaire opposant l'écrivain Pierre Mertens à l'homme politique Bart De Wever, pour des propos que le premier avait tenus à l'égard du second dans le quotidien français *Le Monde* et dans l'hebdomadaire flamand *Knack*, la chambre du conseil de Bruxelles a conclu à la prescription de l'action pénale, en dépit du maintien de la publication des propos incriminés sur le net[688] [689]. L'ordonnance précise à cet égard que « si la persistance de l'article litigieux dans les archives du journal n'est en rien liée à l'inculpé, elle ne peut davantage l'être au délit de presse qui, dès lors, n'est pas un délit continu ».

c. La responsabilité en cascade dans l'univers numérique

180. Introduction. L'imputabilité de la responsabilité se heurte à de nombreux écueils en présence d'un réseau sans frontières, accessible à tous, et sur lequel les rôles des différents acteurs apparaissent flous et évanescents. Ainsi, la délicate question de l'application de la responsabilité en cascade au média numérique a été soulevée à plusieurs reprises en jurisprudence. La difficulté majeure est d'identifier dans l'univers numérique les différents acteurs visés à l'article 25, alinéa 2, de la Constitution (« auteur », « éditeur », « imprimeur », « distributeur »), lequel a été pensé dans le contexte de la presse imprimée. Pour ne rien arranger à l'affaire, et comme il a été relevé en doctrine, le mécanisme constitutionnel de la responsabilité en cascade ne correspond pas au régime d'exonération conditionnelle mis en place par la directive communautaire sur le commerce électronique, notamment au profit de l'hébergeur[690].

181. L'applicabilité du mécanisme à l'internet. L'on ne s'étonnera donc pas, au vu des obstacles susmentionnés, que la jurisprudence soit loin d'être unifiée sur la question de l'applicabilité de la garantie prévue à l'article 25, alinéa 2, de la Constitution aux propos échangés sur le net.

Aux yeux de la cour d'appel de Bruxelles, « le régime de la responsabilité en cascade (…) n'est pas applicable aux intermédiaires des nouveaux réseaux de communications, tels les forums de discussion »[691].

Dès lors, pour la cour, rien ne fait obstacle à l'application au gestionnaire d'un forum de discussion des règles classiques de la participation criminelle : « La responsabilité pénale relative à la diffusion par un internaute d'un texte sur un forum de discussion incombe à son auteur direct, soit à la personne qui a posté le message. Le gestionnaire du forum ne pourrait être poursuivi en qualité de coauteur ou de complice de cet internaute que dans l'un des cas de corréité ou de complicité énumérés limitativement par les articles 66 et 67 du Code pénal, et aux conditions légales desdits cas de figure. Au rang de celles-ci se trouve la volonté de s'associer au même crime ou délit en apportant une aide, indispensable ou simplement utile à sa commission, ou celle de

688 Corr. Bruxelles (ch. cons.), 14 février 2012, *J.L.M.B.*, 2012, p. 817 ; *A&M*, 2012, p. 372.

689 Sur cette question, voy. M. Isgour, « Le délit de presse sur Internet a-t-il un caractère continu ? », note sous Civ. Bruxelles (réf.), 2 mars 2000, *A&M*, 2001, pp. 147-157, qui souligne la nécessité de démontrer la volonté de l'auteur de maintenir son propos pour faire courir un nouveau délai de prescription.

690 Voy., à ce sujet, la contribution d'E. Montero dans la présente chronique. Voy. également B. Van Besien, « La responsabilité des gestionnaires de forums de discussion ''non commerciaux'' », note sous Civ. Anvers (5e ch. B), 3 décembre 2009, *A&M*, 2010, p. 568 ; S. Mampaey et E. Werkers, *op. cit.*, pp. 156-158 ; F. Jongen, « Hiérarchie des normes ? », note sous Corr. Bruxelles, 23 juin 2009, *J.L.M.B.*, 2010, p. 127 ; E. Montero et H. Jacquemin, « La responsabilité civile des médias », vol. 3, in *Responsabilités – Traité théorique et pratique*, Dossier 26*ter*, Bruxelles, Kluwer, 2004, p. 15, n° 184.

691 Bruxelles (12e ch.), 23 janvier 2009, *R.D.T.I.*, 2009, p. 105, note P.-F. Docquir ; *A&M*, 2009, p. 639.

le provoquer par l'un des modes décrits à l'article 66, alinéas 4 et 5, du Code pénal. Le gestionnaire du forum pourrait, par ailleurs, être poursuivi en qualité d'auteur de l'infraction envisagée si, notamment, il a lui-même posté le message délictueux, diffusé ou maintenu en connaissance de cause un message délictueux posté par un tiers identifié ou non, en l'absence même de tout concert préalable avec lui, ou personnellement modifié le message d'un internaute le rendant de la sorte infractionnel »[692].

Dans le même sens, d'après le tribunal correctionnel de Bruxelles, « même si l'auteur et/ou l'éditeur responsable d'un écrit sont connus, la personne responsable d'un site web peut être poursuivie pour le fait d'avoir affiché et continué à afficher l'écrit litigieux sur le site en question »[693].

En revanche, sans analyser la question plus avant, le tribunal de première instance d'Hasselt a estimé que la responsabilité en cascade pouvait trouver à s'appliquer à l'égard d'un journal syndical publié sur l'internet[694].

Dans une autre affaire, l'auteur des propos étant demeuré inconnu, le juge a accepté d'imputer la responsabilité à l'« éditeur » du site mais a refusé d'en faire de même pour le « webmaster » du site au motif que ce dernier n'exerce qu'une fonction purement technique[695].

Une voie médiane a été empruntée par la cour d'appel d'Anvers, pour laquelle la responsabilité en cascade, mise en place à l'article 25, alinéa 2, de la Constitution, « laisse intact le fait que celui qui gère le site Internet sur lequel les articles incriminés sont publiés puisse être tenu responsable sur le terrain de la responsabilité civile[696] »[697]. Il en est ainsi « lorsque l'organisation qui gère le site internet s'identifie au contenu des articles qu'elle a publiés »[698]. On peut penser qu'en s'identifiant aux vues défendues dans les articles, le gestionnaire a acquis la qualité de coauteur et qu'à ce titre, il ne peut plus se décharger de sa responsabilité sur l'auteur des propos litigieux[699].

d. Des devoirs et responsabilités particuliers sur l'internet

182. Plan. Les décisions rendues au cours de la période examinée comportent d'importants développements sur le terrain de la liberté d'expression journalistique et de la liberté de parole en matière politique.

1° Les devoirs et responsabilités journalistiques

183. Introduction. Il est un truisme d'affirmer que les pratiques journalistiques ont connu d'importantes mutations avec l'émergence du média numérique. Ces changements entraînent des

692 *Ibid.*

693 Corr. Bruxelles (61e ch.), 27 novembre 2009, *J.L.M.B.*, 2010, p. 10.

694 Civ. Hasselt (4e ch. A), 14 juin 2010, *A&M*, p. 250, note D. Voorhoof. D'après le tribunal, l'auteur étant resté inconnu, l'éditeur pouvait être poursuivi.

695 Corr. Bruxelles (54e ch.), 23 juin 2009, *J.L.M.B.*, 2010, p. 123, note F. Jongen.

696 Ce faisant, l'arrêt peut laisser penser à tort que la responsabilité en cascade ne concerne que les poursuites pénales. Or, la Cour de cassation a clairement posé que le principe contenu à l'article 25, alinéa 2, trouvait également à s'appliquer en matière civile (Cass (1re ch.), 31 mai 1996, *Pas.*, I., p. 202).

697 Anvers (2e ch.), 23 juin 2010, *A&M*, 2011, p. 223, note D.V. ; *NjW*, 2010, 790, note E.B.

698 *Ibid.*

699 Voy., à ce propos, E. Montero et H. Jacquemin, « La responsabilité civile des médias », *op. cit.*, pp. 9-10, n° 171.

responsabilités spécifiques qui ont trait aussi bien à la collecte qu'à la communication de l'information sur le réseau des réseaux. Ces deux questions seront analysées successivement.

184. L'utilisation d'informations disponibles sur l'internet. L'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *Editorial Board of Pravoye Delo et Shtekel contre Ukraine* est intéressant à plus d'un titre. La Cour de Strasbourg s'y est fendue d'un intéressant *obiter dictum* sur la portée très large du médium numérique et qui mérite d'être reproduit : « L'Internet est certes un outil d'information et de communication qui se distingue particulièrement de la presse écrite, notamment quant à sa capacité à emmagasiner et diffuser l'information. Ce réseau électronique, desservant des milliards d'usagers partout dans le monde, n'est pas et ne sera peut-être jamais soumis aux mêmes règles ni au même contrôle. Assurément, les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée. Aussi, la reproduction de matériaux tirés de la presse écrite et celle de matériaux tirés de l'Internet peuvent être soumises à un régime différent. Les règles régissant la reproduction des seconds doivent manifestement être ajustées en fonction des caractéristiques particulières de la technologie de manière à pouvoir assurer la protection et la promotion des droits et libertés en cause »[700].

Il s'agissait, en l'espèce, de la condamnation d'un journal imprimé à faire paraître une excuse après avoir reproduit dans ses éditions une lettre anonyme diffusée sur un site Internet selon laquelle certains fonctionnaires des services de sécurité se seraient livrés à des activités illégales et à des actes de corruption et entretiendraient des liens avec des membres de groupes criminels.

Le droit ukrainien en vigueur prévoyait une exonération de responsabilité pour les journalistes qui se bornaient à reproduire des matériaux publiés dans d'autres sources *de presse* mais les juridictions nationales avaient exclu de cette immunité les journalistes qui reprenaient des informations publiées sur Internet, à défaut pour ces dernières de constituer des publications enregistrées. Or aucune règle ne prévoyait pareil enregistrement des publications numériques. En dépit des spécificités de l'internet, qui pourraient lui valoir un traitement différencié, la Cour a jugé que l'exclusion totale de ce support de la garantie bénéficiant aux journalistes lorsqu'ils relayent les propos d'autrui constituait un obstacle à l'exercice par la presse de sa fonction essentielle de « chien de garde ».

Cela étant, le journaliste doit faire preuve d'une grande prudence lorsqu'il s'appuie sur des témoignages anonymes[701]. Ainsi, en Belgique, le tribunal de première instance de Bruxelles a souligné les précautions dont doit s'entourer le journaliste qui souhaiterait se fonder sur des commentaires diffusés sur l'internet, précisément en raison de l'impossibilité d'en identifier l'auteur. En conséquence, « si [les réactions] sont susceptibles d'établir un certain contexte de polémique, elles ne peuvent […] asseoir les faits dénoncés dans les articles litigieux, si ce n'est l'existence même de ces réactions »[702].

Par ailleurs, d'après la Cour européenne des droits de l'homme, les journalistes ne sauraient alléguer de la diffusion préalable dans la presse et sur le net d'informations privées concernant le

700 Cour eur. D.H. (5e sect.), 5 mai 2011, arrêt *Comité de rédaction Pravoye Delo et Shtekel contre Ukraine*, § 63.
701 Voy. notamment Civ. Bruxelles (21e ch.), 15 octobre 2009, *A&M*, 2010, p. 202.
702 Civ. Bruxelles (14e ch.), 8 novembre 2011, *A&M*, 2012, p. 261.

comportement d'un mineur et l'identité de ses parents pour justifier l'octroi d'une plus grande publicité à ces renseignements[703].

Dans le même ordre d'idées, le contexte de publication d'une photographie sur le net détermine également la possibilité de son utilisation ultérieure par les journalistes aux fins d'illustrer un article de presse. Une telle conclusion ressort d'une ordonnance de référé rendue par le président du tribunal de première instance de Bruxelles qui a jugé qu'« une personne qui accepte que différentes photographies d'elle comme mannequin soient consultables sur un site internet gratuit et librement accessible à tout un chacun est considérée comme ayant donné son accord tacite quant à l'utilisation des photographies publiées dans d'autres publications *pour autant que les photographies se situent dans un contexte similaire* »[704].

Enfin, la Cour européenne a considéré que l'absence de connexion à l'internet ne pouvait dispenser un journaliste de vérifier des informations par d'autres voies[705].

185. La communication d'informations sur l'internet. La qualité de journaliste d'un internaute pourrait lui valoir une responsabilité accrue lorsqu'il se présente comme tel en s'exprimant sur le réseau.

Dans l'affaire *Fatullayev contre Azerbaijan*, le requérant, journaliste de profession, se plaignait de la condamnation que lui avaient value des propos prétendument diffamatoires tenus sur un forum de discussion[706]. Les affirmations prêtées au requérant accusaient des soldats azéris non identifiés d'avoir tiré en direction de leurs propres civils et d'avoir mutilé leurs cadavres durant le conflit du Haut-Karabagh opposant l'Azerbaïdjan et l'Arménie[707]. Le requérant avait toujours nié être l'auteur des propos litigieux et prétendu avoir été la victime d'un imposteur. La Cour a estimé, quant à elle, que la paternité de l'auteur quant aux déclarations litigieuses avait été prouvée « au-delà du doute raisonnable »[708].

La Cour commença par rappeler les devoirs et responsabilités qui incombent aux journalistes[709]. Elle releva, ensuite, que « restait irrésolue la question de savoir si le requérant avait l'intention de poster ses commentaires en sa qualité de journaliste délivrant de l'information au public, ou s'il avait simplement exprimé ses opinions personnelles, comme un citoyen ordinaire, dans le cadre d'un débat ayant cours sur Internet »[710]. Néanmoins, d'après les juges strasbourgeois, en intervenant sous nom, « le requérant, un journaliste célèbre, n'avait rien fait pour cacher son identité et il avait diffusé publiquement ses allégations en les postant sur un forum Internet populaire

703 Cour eur. D.H. (1re sect.), 16 décembre 2010, arrêt *Aleksey Ovchinnikov contre Russie*, §§ 49-52.

704 Civ. Bruxelles (prés.), 22 octobre 2009, *A&M*, 2010, p. 301 et note. Nous soulignons.

705 Cour eur. D.H. (4e sect.), 22 novembre 2011, arrêt *Koprivica c. Monténégro*, § 69.

706 Cour eur. D.H. (1re sect.), 22 avril 2010, arrêt *Fatullayev contre Azerbaijan*.

707 § 94.

708 *Ibid.*, § 93.

709 § 95.

710 *Ibid.*, § 95. Traduction libre : « In the present case, it is not clear whether the applicant intended to post these statements in his capacity as a journalist providing information to the public, or whether he simply expressed his personal opinions as an ordinary citizen in the course of an Internet debate ».

librement accessible, un médium qui, dans les temps modernes, n'a pas un effet moins puissant que les médias imprimés »[711].

Dans le même ordre d'idées, le Conseil de déontologie journalistique[712] a estimé à travers un avis général que « (…) les personnes exerçant une activité d'information, comme tout individu, ont droit à une sphère d'expression privée. Mais lorsqu'elles diffusent des messages d'information sur un support numérique destiné à un public non défini et non limité, il faut considérer qu'elles y exercent une activité de type journalistique. Elles sont par conséquent tenues d'y respecter leur déontologie professionnelle »[713].

2° La liberté d'expression politique

186. Introduction. Durant la période examinée, la Cour de Strasbourg a rendu trois arrêts importants mettant en cause la liberté d'expression d'hommes politiques ou de militants ayant eu recours au médium numérique pour répandre leurs idées et opinions.

187. L'étendue de la liberté d'expression politique. Dans un arrêt *Renaud contre France*, la Cour européenne a jugé disproportionnée la condamnation d'un militant du chef de diffamation et d'injure publiques à raison d'invectives proférées contre le maire de sa commune sur le site Web de son association et dénonçant certains projets urbanistiques. En dépit de la virulence des propos litigieux, la Cour a relevé que « même s'ils ne s'inscrivent pas dans le cadre de la liberté d'expression d'un membre de l'opposition à proprement parler, ces propos relèvent de l'expression de l'organe représentant d'une association portant les revendications émises par ses membres sur un sujet d'intérêt général dans le cadre d'une politique municipale »[714]. La Cour a par ailleurs observé que « le requérant, engagé dans la vie politique locale, ainsi qu'en atteste notamment son élection ultérieure, s'inscrivait dans une démarche d'opposition politique »[715].

188. Les limites à la liberté d'expression politique. Pour autant, même sur le terrain politique, la liberté d'expression n'est pas sans limites. Ainsi dans l'arrêt *Féret contre Belgique*, une majorité de juges strasbourgeois a estimé conforme à l'article 10 la condamnation d'un homme politique belge pour avoir incité à la haine et à la discrimination raciale, notamment par le biais d'un site Web[716]. Dans leur opinion dissidente, les juges minoritaires ont pourtant mis l'accent sur le caractère peu « invasif » du médium numérique : « Il est exact que certains documents étaient disponibles en même temps (quoique séparément) sur le site web de M. Féret mais les sites web se distinguent d'autres formes de distribution parce qu'on peut les ''télécharger'' à son gré (les intéressés doivent rechercher eux-mêmes activement l'information). Autrement dit, les opinions

711 *Ibid.*, § 95. Nous traduisons : « Nevertheless, it is clear that, by posting under the username 'Eynulla Fatullayev', the applicant, being a popular journalist, did not hide his identity and that he publicly disseminated his statements by posting them on a freely accessible popular Internet forum, a medium which in modern times has no less powerful an effect than the print media ».

712 On rappellera, si besoin en est, que les prises de position du Conseil de déontologie journalistique ne bénéficient que d'une autorité morale.

713 Conseil de déontologie journalistique, *Avis sur l'application de la déontologie journalistique aux réseaux sociaux*, 13 octobre 2010. Disponible sur le site www.deontologiejournalistique.be.

714 Cour eur. D.H. (5e sect.), 25 février 2010, arrêt *Renaud contre France*, § 40.

715 *Ibid.*, § 40.

716 Cour eur. D.H. (2e sect.), 16 juillet 2009, arrêt *Féret c. Belgique*.

ne sont pas ''imposées'' comme elles le sont lors de la divulgation de documents papier »[717]. De la même manière, aux yeux de la Cour (ou du moins d'une large majorité des juges qui composaient la chambre saisie), l'appel au boycott de produits en provenance d'Israël lancé au cours d'une réunion du conseil municipal et repris sur Internet pouvait justifier la condamnation d'un maire pour incitation à la discrimination, en dépit du fait qu'il fût motivé par la politique menée par le premier ministre de ce pays[718].

e. Le droit de réponse en ligne et la contradiction des propos diffusés en ligne

189. La notion d'« écrit périodique ». En l'absence de législation réglementant spécifiquement les modalités d'exercice d'un droit de réponse en ligne[719], les juges belges ont « bricolé » des solutions originales en partant de la notion d'« écrit périodique » mentionnée à l'article 1er de la loi du 23 juin 1961 relative au droit de réponse[720].

Ainsi, le tribunal de première instance de Bruxelles a considéré que : « Attendu que la loi du 23 juin 1961 dans son chapitre 1, ici concerné, s'applique aux écrits périodiques ; Que, cependant, la loi ne définit pas ce qu'il convient d'entendre par ces termes ; Que, notamment, elle n'a pas précisé que les écrits périodiques en question devaient exclusivement être imprimés sur du papier. Attendu que le journal *La Libre Belgique* où furent publiés les articles litigieux, est également et concomitamment publié sur son site internet où des abonnés peuvent le consulter. Que les articles dans lesquels le demandeur est cité ont été publiés sur ce site, tels quels ou légèrement adaptés, et ont pu être lus tout comme la version papier du journal ; Attendu, par conséquent que rien ne permet de considérer que la partie de la loi concernant les écrits périodiques ne devrait ou ne pourrait pas s'appliquer aux reproductions d'articles sur le site internet desdits périodiques »[721].

Dans le même sens, il a également été jugé que « l'on pourrait admettre, en théorie, qu'un site web régulièrement mis à jour sur internet, puisse être considéré comme un écrit périodique au sens de l'article 1er de la loi du 23 juin 1961 relative au droit de réponse et donner ouverture au recours spécifique prévu par l'article 12 de ladite loi »[722].

---

717 Opinion dissidente du juge Sajó à laquelle se rallient les juges Zagrebelsky et Tsotsoria.

718 Cour eur. D.H. (5e sect.), 16 juillet 2009, arrêt *Willem contre France*. Voy. cependant l'opinion dissidente du juge Jungwiert jointe à cet arrêt.

719 En dépit d'une recommandation du Comité des ministres du Conseil de l'Europe (Recommandation Rec(2004)16 du Comité des ministres aux États membres sur le droit de réponse dans le nouvel environnement des médias, adoptée le 15 décembre 2004, lors de la 909e réunion des Délégués des ministres), d'une proposition de loi déposée sur le bureau du Sénat (proposition de loi modifiant la loi du 23 juin 1961 relative au droit de réponse, déposée par Mme C. Defraigne, 30 septembre 2010, *Doc. parl.*, Sénat, sess. extraord., 2010, no 5-196/1, et déjà déposée le 28 mai 2009, *Doc. parl.*, Sénat, sess. ord., 2008-2009, no 4-1347/1), et de nombreuses suggestions doctrinales (voy. notamment P.-F. Docquir, « Le ''Droit de réponse 2.0'' ou la tentation d'un droit subjectif d'accès à la tribune médiatique », *Rev. dr. ULB*, 1/2007, pp. 289-313 ; H. Jacquemin, E. Montero et S. Pirlot de Corbion, « Le droit de réponse dans les médias », *R.D.T.I.*, 2007, pp. 31-66).

720 Loi relative au droit de réponse, *M.B.*, 8 juillet 1961. Cette solution avait déjà été avancée en doctrine, quoiqu'avec certaines réserves. Voy. F. Jongen, « Le droit de réponse dans la presse et l'audiovisuel », in A. Strowel et F. Tulkens (dir.), *Prévention et réparation des préjudices causés par les médias*, Bruxelles, Larcier, 1998, pp. 55-56.

721 Corr. Bruxelles (44e ch.), 30 octobre 2009, *A&M*, 2010, p. 571.

722 Civ. Bruxelles (14e ch.), 13 avril 2010, *A&M*, 2010, p. 579.

190. La publication d'un avis rectificatif. Sans passer par la législation sur le droit de réponse, le président du tribunal de première instance d'Anvers a admis, quant à lui, qu'« en réaction à un article sur un site Internet d'actualités, il peut être enjoint à la personne morale responsable de publier un avis rectificatif, sous peine d'astreintes par jour de retard »[723]. En revanche, le juge a déclaré non fondée l'action en suppression de l'article[724].

191. La publication du jugement. Le tribunal de première instance de Bruxelles a fait droit à la demande d'une entreprise, dont la réputation avait été fautivement ternie par un journaliste, d'ordonner la publication du jugement dans l'édition papier et ainsi que sur le site Internet du magazine « pendant une première période de quinze jours et ensuite aussi longtemps que l'article litigieux reste consultable »[725].

IV. 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[726]

A. Introduction

192. Propos introductifs sur l'objet des décisions recensées. L'essentiel de la jurisprudence examinée en matière de droit au respect de la vie privée lié à l'utilisation des NTIC dans les relations de travail a été rendu dans des litiges opposant employeurs et travailleurs à propos de la régularité d'un licenciement pour motif grave[727]. C'est dans le cadre de la production d'éléments de preuve destinés à établir le motif du licenciement (qu'il soit ou non fondé sur l'usage de ces technologies), que se noue le débat sur l'existence ou non d'une violation des dispositions qui consacrent et organisent une protection de la vie privée du travailleur sur le lieu du travail.

La problématique ne concerne donc pas tant l'usage éventuellement abusif d'outils mis à la disposition du travailleur (par exemple téléchargement illégal, consultation de sites pornographiques) mais, dans la plupart des décisions consultées, plutôt le sort à réserver à des preuves issues de l'utilisation des NTIC (*e-mails*, documents stockés sur CD-Rom ou sur un disque dur, données de géolocalisation, enregistrement audio ou vidéo, production de SMS ou encore informations glanées sur Facebook, etc.), et qui sont susceptibles d'établir l'existence d'une faute dans le chef du travailleur. Nous examinerons les enseignements de la jurisprudence concernant les conditions dans lesquelles il y a ou non méconnaissance des dispositions légales applicables en rapport avec l'usage de différentes technologies (B, *infra*).

723 Civ. Anvers (prés.), 24 novembre 2010, ordonnance précitée.

724 Voy. *supra* sur ce point.

725 Civ. Bruxelles (14e ch.), 8 novembre 2011, jugement précité.

726 Assistante à la faculté de droit des FUNDP. Chercheuse au Centre de Recherche Informatique, Droit et Société (CRIDS), Université de Namur. Avocate au barreau de Namur.

727 Pour la jurisprudence rendue par la Cour européenne des droits de l'homme concernant l'application de l'article 8 de la C.E.D.H. dans les relations de travail, voy. la contribution de J. Herveg relative à la jurisprudence de la Cour européenne de Strasbourg, pp. 99 et s., et notamment les nos 147, 153 et 157.