Criminalité informatique

Delhaise, Elise; Knockaert, Manon; Lachapelle, Amelie

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2021

Document Version
le PDF de l'éditeur

VI. CRIMINALITÉ INFORMATIQUE

Elise Delhaise[977], Manon Knockaert[978] et Amélie Lachapelle[979]

304. Plan des développements. Cette partie de la chronique examine les décisions rendues entre le 1er janvier 2018 et le 31 décembre 2020 dans le domaine de la criminalité et du numérique.

Nous analysons la jurisprudence belge et européenne rendue en matière de droit pénal matériel (A), de mesures d'instruction et d'information (B), d'obligations de collaboration (C) et de dispositifs de surveillance (D). Au vu du récent arrêt prononcé par la Cour européenne des droits de l'homme dans le cadre de l'affaire « *Lux Leaks* »[980], il nous a paru intéressant de revenir brièvement, dans le cadre de la présente chronique, sur cette affaire dès lors que le juge luxembourgeois a reconnu, à cette occasion, le fait justificatif « du lanceur d'alerte » (E).

A. Infractions liées à l'environnement numérique

1. Infractions à caractère sexuel

a. Attentat à la pudeur et possession d'images pédopornographiques

305. La possession d'images à caractère pédopornographique. Par un arrêt du 28 février 2018[981], la Cour de cassation se prononce sur la portée de l'article 383*bis* du Code pénal. L'affaire porte sur la condamnation d'un prévenu pour possession et conservation de photographies d'enfants nus, notamment dans le cadre de pratiques sportives en milieu naturiste, à des fins principalement sexuelles[982]. Outre une violation du principe de légalité[983], le prévenu reproche à la juridiction de fond une interprétation extensive de l'article 383*bis* du Code pénal. En effet, la juridiction d'appel a décidé qu'était couverte par cette disposition la conservation de clichés comportant notamment des sexes d'enfants à des fins principalement sexuelles. Or, d'après le demandeur, l'incrimination vise uniquement la représentation des organes sexuels d'un enfant[984].

977 Assistante-doctorante à l'UNamur.

978 Chercheuse au CRIDS.

979 Chargée d'enseignement à l'UNamur et chercheuse senior au CRIDS.

980 Cour eur. D.H. (3e sect.), arrêt *Halet c. Luxembourg*, 11 mai 2021, req. no 21884/18.

981 Cass. (2e ch.), 28 février 2018, *Pas.*, 2018, p. 476.

982 La saisie du matériel informatique du prévenu a notamment dévoilé la consultation de sites web montrant des photographies d'enfants dénudés ainsi qu'un accord avec un tiers en vue de l'échange d'images montrant de jeunes garçons se livrant à des jeux sexuels ainsi que le versement d'argent pour réaliser de telles photographies.

983 Notons que la Cour de cassation décide que ce moyen manque en droit et en fait, précisant que le principe de légalité ne s'oppose pas à ce que la loi attribue un pouvoir d'appréciation au juge.

984 Cass. (2e ch.), 28 février 2018, *Pas.*, 2018, pp. 479-480. Au moment des faits, l'article 383*bis* du Code pénal disposait que : « Sans préjudice de l'application des articles 379 et 380, quiconque aura exposé, vendu, loué, distribué, diffusé ou remis des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou fait importer, remis à un agent de transport ou de distribution, sera puni de la réclusion de cinq ans à dix ans et d'une amende de cinq cents [euros] à dix mille [euros] ». La loi du 31 mai 2016 (loi du 31 mai 2016 complétant la mise en œuvre des obligations européennes en matière d'exploitation sexuelle des enfants, de pédopornographie, de traite des êtres humains et d'aide à l'entrée, au transit et au séjour irréguliers, *M.B.*, 8 juin 2016, p. 34574.) complète l'infraction en incriminant quiconque a « sciemment et sans droit (…) possédé du matériel pédopornographique (…) ». L'on retrouve, à l'origine de cette modification législative, la directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus

La Cour de cassation relève que le second paragraphe de l'article 383*bis* du Code pénal dispose que « [q]uiconque aura sciemment et sans droit acquis, possédé du matériel pédopornographique ou y aura, en connaissance de cause, accédé par le biais des technologies de l'information et de la communication, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent euros à mille euros ». Si l'acte de possession est visé, encore faut-il déterminer la portée de la notion de « contenu pédopornographique ». À cet égard, le quatrième paragraphe adopte une interprétation large de la notion de matériel pédopornographique. Rentre notamment dans la définition le matériel représentant de manière visuelle, par quelque moyen que ce soit, un mineur ou une personne paraissant être un mineur, se livrant à un comportement sexuellement explicite, réel ou simulé, ou représentant ses organes sexuels[985]. Sur la base de ces éléments, la Cour de cassation suit le raisonnement des juges d'appel et décide que le moyen manque en fait[986].

b. Viol « à distance »

306. Viol par auto-pénétration réalisée sous l'effet de menaces exercées via les réseaux sociaux. Il ressort d'un jugement du tribunal correctionnel francophone de Bruxelles[987] que l'infraction de viol ne nécessite pas un contact physique. En l'occurrence, un acte d'auto-pénétration réalisé sous l'effet de menaces exercées via le réseau social *Facebook* peut donc répondre à la qualification de viol[988]. Le tribunal constate *in casu* que les éléments constitutifs du viol sont présents. Premièrement, l'acte de (auto)pénétration sexuelle est démontré par les messages échangés entre la victime et le prévenu sur le réseau social, et par les captures d'écran de la vidéo retrouvées sur le téléphone de ce dernier. Se référant aux travaux préparatoires de la loi ayant inséré la prévention de viol dans le Code pénal, le tribunal relève qu'est visée la pénétration par « quelque moyen »[989], jugeant ainsi que l'infraction « inclut dès lors l'hypothèse dans laquelle une personne est contrainte d'accomplir une pénétration sexuelle sur sa propre personne alors même qu'aucun contact physique avec la personne qui l'y contraint n'ait lieu »[990]. Troisièmement, le juge reconnaît le défaut de consentement dans le chef de la victime par une appréciation *in concreto* des circonstances de l'espèce. L'âge de la victime (15 ans) ainsi que le chantage exercé par le prévenu ont été déterminants pour révéler la contrainte morale et la ruse employée pour

sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie. Le considérant 9 précise que « la pédopornographie (…) peut (…) comporter des images d'enfants participant à un comportement sexuellement explicite ou des images de leurs organes sexuels, lorsque ces images sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non ».

985 Cass. (2e ch.), 28 février 2018, *Pas*., 2018, pp. 480-481.

986 Cass. (2e ch.), 28 février 2018, *Pas*., 2018, p. 481.

987 Corr. Bruxelles (54e ch.), 25 septembre 2018, *J.L.M.B*., 2019/14, pp. 653-656.

988 Au moment des faits, l'infraction de viol incriminée à l'article 375 du Code pénal était libellée comme suit : « [t]out acte de pénétration sexuelle, de quelque nature qu'il soit et par quelque moyen que ce soit, commis sur une personne qui n'y consent pas, constitue le crime de viol. Il n'y a pas consentement notamment lorsque l'acte a été imposé par violence, contrainte ou ruse, ou a été rendu possible en raison d'une infirmité ou d'une déficience physique ou mentale de la victime ». Depuis l'entrée en vigueur de la loi du 1er février 2016 modifiant diverses dispositions en ce qui concerne l'attentat à la pudeur et le voyeurisme (*M.B*., 19 février 2016), l'article 375 ajoute la menace et la surprise comme défaut de consentement.

989 Proposition de loi modifiant certaines dispositions relatives au crime de viol, *Doc. parl.*, Ch. repr., sess. ord. 1981-1982, no 166, Amendement no 2, p. 2.

990 Corr. Bruxelles (54e ch.), 25 septembre 2018, *J.L.M.B*., 2019/14, p. 654.

intimider, effrayer et forcer la victime à accomplir un acte d'auto-pénétration sexuelle qu'elle ne désirait pas[991].

c. Diffusion d'images d'une personne dénudée sans son consentement

307. Diffusion de photographies sur Internet. Dans un arrêt du 29 octobre 2019, la Cour de cassation précise les conditions d'application de l'article 371/1, alinéa 1er, 2°, du Code pénal qui incrimine le fait de montrer, rendre accessible ou diffuser des images ou l'enregistrement visuel ou audio d'une personne dénudée ou se livrant à une activité sexuelle explicite, sans son accord ou à son insu, même si cette personne a consenti à leur réalisation[992].

En l'espèce, un jeune homme s'était suicidé suite au partage, par le demandeur en cassation, de photographies de lui dénudé sur un compte *Instagram* spécialement dédié à cette fin. Les photographies étaient accompagnées d'un commentaire dénigrant mentionnant son nom. D'après le demandeur en cassation, la diffusion en tant que telle de photographies sur les réseaux sociaux ne porte pas atteinte au droit à la vie privée des personnes concernées. Le fait qu'une photographie soit, comme en l'espèce, attribuée à une personne déterminée ne signifie pas que cette personne est *reconnaissable* par des tiers, et partant «identifiable» au sens de l'article 371/1 du Code pénal[993]. La Cour de cassation ne souscrit néanmoins pas à cette argumentation, rappelant que l'incrimination pénale, conformément à sa *ratio legis*, a pour but de protéger non seulement la vie privée et l'intimité sexuelle, mais aussi l'intégrité sexuelle[994]. Il s'ensuit que la possibilité d'identifier la victime sur la base d'une image ou d'un enregistrement sonore, rendu accessible ou diffusé, ne constitue nullement un élément constitutif de l'infraction. Or, le droit pénal étant d'interprétation stricte, il n'appartient pas au juge d'ajouter des conditions à l'établissement d'une infraction[995].

d. Corruption de la jeunesse via un avatar

308. Attentat à la pudeur et victime virtuelle. Le 9 juillet 2018, le tribunal correctionnel de Liège se prononce sur l'utilisation d'un avatar pour dénoncer des actes de corruption de la jeunesse[996]. Les faits remontent en 2013, lorsque l'association «Terre des hommes» effectue une enquête portant sur les abus sexuels dont sont victimes les enfants via *webcam*. Pour ce faire, l'association a recours à un avatar représentant une jeune fille de 10 ans proposant un spectacle à la caméra, avec une prétendue petite sœur, en utilisant Skype comme moyen de communication et contre rémunération. Le 10 avril 2014, les services de police belge sont informés d'une conversation entretenue par le prévenu avec l'avatar[997].

991 *Ibid.*, p. 655.

992 Cass. (2e ch.), 29 octobre 2019, R.G. n° P.19.0800.N, *R.A.B.G.*, 2020, p. 668; *T. Straf.*, 2020/3, p. 210; *R.W.*, 2019-20/42, p. 1668 avec note; *J.D.J.*, 2020, n° 395, p. 45.

993 Cass. (2e ch.), 29 octobre 2019, *R.A.B.G.*, 2020, n° 8, p. 669.

994 Voy. not. J. Beyens et E. Lievens, «Niet-consensuele verspreiding van seksuele beelden. Analyse van wetgevende initiatieven in de Verenigde Staten, het Verenigd Koninkrijk en België», *N.J.W.*, 19 octobre 2016, n° 348, 664.

995 L. Delbreouck et L. Neskens, «Intimiteit is niet begrensd door identiteit», *R.A.B.G.*, 2020, n° 8, p. 671.

996 Corr. Liège, div. Liège (19e ch.), 9 juillet 2018, *J.L.M.B.*, 2019, p. 643, note S. Royer, «Le droit pénal belge face à l'intelligence artificielle: de l'appréhension par le droit pénal belge d'un avatar».

997 Corr. Liège, div. Liège (19e ch.), 9 juillet 2018, *J.L.M.B.*, 2019, p. 643.

L'affaire portait sur la notion de mineur d'âge au sens de l'article 379 du Code pénal. Le tribunal rappelle que le droit pénal est d'interprétation stricte, ne permettant dès lors pas de reconnaître qu'un adulte qui se prétend mineur d'âge serait un mineur d'âge[998]. D'après le juge, la prévention de corruption de la jeunesse ne peut être établie, et celui-ci décide donc que « le prévenu a été confronté à un adulte se présentant comme un mineur d'âge mais pas à une victime dans un état de minorité ».[999]

2. Cyberviolence lors d'une procédure en divorce

309. Obligation positive tirée du droit à la vie privée et violence conjugale. La Cour européenne des droits de l'homme a été invitée à se prononcer sur des actes de violences conjugales et de cyberviolence entre ex-époux[1000]. En procédure de divorce, la plaignante accuse son ex-époux de violences domestiques et de violation de sa correspondance et demande une perquisition de l'ordinateur familial. Le but poursuivi est de faire constater par les autorités roumaines une consultation, par son ex-époux, de ses comptes électroniques (notamment, son compte *Facebook*). En outre, la plaignante veut prouver que son ex-époux a copié ses conversations privées, ses documents et ses photos. En l'espèce, les autorités nationales n'ont pas accédé à la demande de perquisition de la partie demanderesse pour deux motifs principaux[1001]. Premièrement, les autorités nationales estiment que les preuves pouvant être recueillies de cette manière seraient sans relation directe avec les accusations de violences domestiques. Aux yeux de la Cour, toutefois, la « cyberviolence » – à savoir les violations informatiques de la vie privée, l'intrusion dans les comptes électroniques de la victime et la prise, le partage et la manipulation des données et des images – fait partie intégrante des violences domestiques à l'ère d'une société marquée par les nouvelles technologies et les réseaux sociaux[1002]. Deuxièmement, les autorités nationales considèrent que les données de la plaignante sont des données publiques dans la mesure où elles peuvent être trouvées sur le réseau social américain. À cet égard, outre que la plainte ne concernait pas uniquement l'utilisation du compte créé sur *Facebook*, la Cour européenne des droits de l'homme insiste sur l'importance et la nécessité d'un véritable examen sur le fond afin de pouvoir appréhender de manière globale le phénomène de violences conjugales « dans toutes ses formes »[1003]. La Cour européenne des droits de l'homme condamne donc l'État pour manquement à ses obligations positives au regard des articles 3 et 8 de la Convention européenne des droits de l'homme[1004].

3. Droit de curiosité entre époux

310. Droit de curiosité et accès au réseau social du conjoint. Nos juridictions belges ont également eu à connaître de l'utilisation du numérique dans les relations conjugales. Par un arrêt

998 *Ibid.*, p. 644.

999 *Ibid.*, p. 644. En revanche, deux autres préventions de corruption de la jeunesse et de détention de photos pédopornographiques ont été déclarées établies. Par ailleurs, le prévenu et le ministère public ont interjeté appel de cette décision.

1000 Cour eur. D.H., arrêt *Buturugă c. Roumanie*, 11 juin 2020, req. n° 56867/15.

1001 *Ibid.*, §§ 5 et s.

1002 *Ibid.*, § 74.

1003 *Ibid.*, §§ 75 et s.

1004 Pour un commentaire de cet arrêt, voy. not. S. Wattier, « La violation du secret de la correspondance et la cyberviolence constituent une forme de violence domestique », *R.D.T.I.*, 2020/1, n° 78, pp. 126-131.

du 28 juin 2018, le tribunal de première instance de Gand[1005] décide que la correspondance papier et électronique, qui n'est pas couverte par le secret professionnel ou qui n'a pas été obtenue de manière illicite, peut être utilisée par un (ancien) conjoint dans le cadre du droit dit « de curiosité » lors d'une procédure de divorce. Le tribunal précise que l'information doit avoir été obtenue *pendant le mariage*, c'est-à-dire jusqu'au jour où la vie conjugale prend fin[1006]. Selon le juge, ledit droit à la curiosité permet de prendre connaissance des lettres reçues par le conjoint. En outre, ni l'article 8 de la Convention européenne des droits de l'homme, ni les articles 22 et 29 de la Constitution, ne s'opposent à leur utilisation dans le cadre d'une procédure en divorce[1007]. Un raisonnement similaire s'applique à la correspondance électronique. Par ailleurs, le juge reconnait *in casu* un exercice proportionné du droit à la curiosité, notamment en raison de l'accessibilité du mot de passe donnant accès au compte *Facebook* de l'épouse et au motif que cet accès a été exercé pendant la période de vie conjugale[1008].

311. Droit de curiosité et violation de la correspondance électronique. Plus récemment, dans un arrêt du 6 septembre 2019, la cour d'appel de Bruxelles[1009] consacre également le droit à la curiosité entre époux. Elle estime ainsi que le droit à la vie privée entre époux, chacun devant respecter la part d'intime qui revient à l'autre, doit être mis en balance avec le droit à la curiosité entre conjoints. D'après la juridiction d'appel, « le droit au respect de la vie privée doit être tempéré par un droit sain à la curiosité pourvu que ce dernier ne soit pas exercé de façon disproportionnée », admettant ainsi la prise de connaissance de courriers électroniques et de SMS par un des époux afin de prouver une relation extraconjugale[1010].

4. Mise à disposition gratuite d'œuvres contrefaites sur des sites de torrent

312. *Torrenting.* Dans un jugement du 14 mai 2018, le tribunal correctionnel de Dendermonde s'est penché sur une situation devenue commune dans l'environnement numérique : des individus ont enregistré via leur décodeur des émissions de télévision et les ont ensuite converties, notamment via le programme *Handbrake*, dans le but de les mettre à disposition gratuitement, grâce entre autres aux programmes *Azareus Bittorent*, *Utorrent*, sur des sites de *torrent*[1011].

313. Délit de contrefaçon. Les œuvres copiées par les deux prévenus étant protégées par le droit d'auteur, ces derniers sont, tout d'abord, poursuivis pour délit de contrefaçon, visé à l'article XI.293, alinéa 1er, du Code de droit économique[1012]. Le délit de contrefaçon requiert un dol

1005 Trib. Gand, 28 juin 2018, *T.G.R.*, 2018/4, pp. 272-274.

1006 Trib. Gand, 28 juin 2018, *T.G.R.*, 2018/4, p. 273. Pour une approche plus nuancée du droit à la curiosité, voy. F. Aps, « Le droit au respect de la vie privée à l'épreuve de l'utilisation d'une correspondance confidentielle dans une procédure en divorce et en ordonnance de mesures provisoires », *J.L.M.B.*, 2000/28, p. 1198 ; B. Allemeersch et S. Ryelandt, « Licéité de la preuve en matière civile : un clone pour "Antigoon" », *J.T.*, 2012, p. 165.

1007 Trib. Gand, 28 juin 2018, *T.G.R.*, 2018/4, p. 273.

1008 *Ibid.*, pp. 273-274.

1009 Bruxelles (43e ch.), 6 septembre 2019, *J.L.M.B.*, 2019, n° 41, p. 1965.

1010 En revanche, se basant sur un arrêt de la Cour de cassation du 17 novembre 2015, la cour d'appel de Bruxelles refuse de prendre connaissance des enregistrements effectués par l'ex-épouse à l'insu de Monsieur car elle considère qu'il y a une atteinte inacceptable au respect de la vie privée protégée par l'article 8 de la Convention européenne des droits de l'homme ; Bruxelles (43e ch.), 6 septembre 2019, *J.L.M.B.*, 2019, n° 41, p. 1968.

1011 Corr. Dendermonde, 14 mai 2018, *A&M*, 2018-2019/1, pp. 80-87.

1012 La loi du 30 juin 1994 a été abrogée par la loi du 19 avril 2014, mais les faits visés par les infractions établies par cette loi demeurent punissables en vertu des articles XI.215, qui protège le droit des organismes de radiodiffusion sur leurs

spécial, à savoir une intention frauduleuse ou méchante. S'il est plus difficile d'établir l'intention méchante, qui suppose de chercher à offenser moralement l'auteur, il ne fait ici pas de doute que les prévenus étaient mus par une intention frauduleuse, en ce qu'ils cherchaient à se procurer, pour eux-mêmes ou pour autrui un avantage économique illégal en convertissant les fichiers téléchargés dans leur propre format, puis en les rendant disponibles gratuitement sur des sites de *torrents*[1013].

314. Fraude informatique. Le *torrenting* peut également être sanctionné sur pied de l'article 504*quater* du Code pénal qui réprime l'infraction de fraude informatique. La fraude informatique consiste dans le fait de chercher à se procurer, pour soi-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique. Dès lors que l'accès aux programmes télévisés visés par l'infraction est payant, l'intention frauduleuse est établie. Partant, l'infraction de fraude informatique est en l'espèce établie[1014].

315. Faux en informatique. L'infraction de faux en informatique consiste dans un comportement similaire à celui de fraude informatique. Il s'en distingue néanmoins dans son but qui est, conformément à l'article 210*bis*, § 1er, du Code pénal, de modifier la portée juridique des données informatiques. Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux sur pied de l'article 210*bis*, § 2, du Code pénal. La modification de la portée juridique consiste, dans l'affaire examinée par le tribunal correctionnel de Dendermonde, dans la mise à disposition gratuite et souvent prématurée de programmes qui ne peuvent, en règle, être consultés que moyennant paiement au moment et au lieu décidés par l'auteur[1015].

316. Hacking externe. D'après l'article 550*bis*, § 1er, du Code pénal, le *hacking* externe consiste dans l'accès illégal à tout ou partie d'un système informatique, ou son maintien, par des personnes qui savent ne pas y être autorisées. L'infraction suppose donc la réunion de deux éléments : un élément matériel (accès ou maintien illégal) et un élément moral (dol général). Il découle de l'article 550*bis*, § 1er, alinéa 2, du Code pénal que le fait de commettre l'infraction avec une intention frauduleuse constitue une circonstance aggravante. Le même article sanctionne également, en son septième paragraphe, le recel de données « hackées », autrement dit obtenues illégalement. Il découle des considérations exposées plus haut que les trois infractions sont établies en l'espèce[1016].

émissions de télévision, et de l'article XI.293, alinéa 1er, du CDE, qui prévoit le délit de contrefaçon. Cette remarque est importante puisqu'un acte d'accusation porte sur une période s'étendant du 1er juillet 2012 au 31 décembre 2014 inclus.

1013 Corr. Dendermonde, 14 mai 2018, *A&M*, 2018-2019/1, point 8 du jugement.

1014 *Ibid.*, point 10 du jugement.

1015 *Ibid.*, point 12 du jugement.

1016 *Ibid.*, point 14 du jugement.

317. Harcèlement par des moyens de communications électroniques. Enfin[1017], le juge a considéré que le comportement des prévenus était également sanctionnable pénalement, sur la base de l'article 145, § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques qui punit le fait d'utiliser un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages. L'infraction suppose donc un dol spécial qui consiste dans le fait soit de vouloir importuner son correspondant, soit de vouloir provoquer des dommages. En l'espèce, les deux prévenus ont provoqué, par leur comportement, des dommages aux auteurs des programmes de télévision[1018].

B. Instruction et information dans l'environnement numérique

1. Écoutes téléphoniques

a. Proportionnalité des méthodes de recherche

318. Contrôle visuel discret et observation systématique à l'aide de moyens techniques. La Cour de cassation a rappelé dans son arrêt du 4 novembre 2020[1019] que le contrôle visuel discret (article 46*quinquies* C.i.cr.) et l'observation systématique à l'aide de moyens techniques (article 47*sexies*, § 2, C.i.cr.) sont soumis au respect d'une condition de proportionnalité. Ainsi, des indices sérieux sont requis pour la mise en œuvre de ces deux méthodes d'enquête.

Dans ce cadre, le demandeur contestait que la chambre des mises en accusation ait validé, par son arrêt du 23 octobre 2020, des méthodes non valablement autorisées car fondées sur de simples suspicions et non des indices sérieux. La Cour souligne que « les indices sérieux de culpabilité dans le chef d'un suspect » sont à distinguer de « l'exigence d'une proportionnalité entre la méthode de recherche utilisée et la gravité de l'infraction visée ». Il ne faut dès lors pas confondre culpabilité de l'auteur et mise en œuvre des méthodes d'enquête permettant justement d'apporter des éléments de preuve à l'appui de la culpabilité de l'auteur. Le moyen n'a, par conséquent, pas été accueilli par la Cour.

b. Respect du droit à la vie privée

319. Interception des communications et persistance de la violation de l'article 8 de la CEDH. Dans son arrêt *Bivolaru contre Roumanie* (n° 1)[1020], la Cour européenne des droits de l'homme a reconnu l'existence d'une atteinte au droit au respect de la vie privée du requérant en raison de l'interception de ses communications. Ce même requérant saisit une nouvelle fois

[1017] Même si cette prévention ne suppose pas de recourir à des technologies de l'information, notons que le tribunal a également considéré que les deux prévenus faisaient partie d'une bande au sens de l'article 322 du Code pénal (point 16). Le seul fait de l'organisation est sanctionné pénalement, même sans passage à l'acte.

[1018] *Ibid.*, point 18 du jugement. Compte tenu de la gravité et de l'étendue des faits, les deux prévenus sont condamnés à un an d'emprisonnement et à une peine d'amende. Leur casier judiciaire étant vierge, le juge prononce cependant le sursis à l'exécution pour toute la durée de l'emprisonnement et la suspension partielle de l'amende. Les demandes d'indemnisation des parties civiles (VRT, SBS Belgium et Medialaan) ont par ailleurs été admises et déclarées fondées sur la base des articles 1382 et 1388 du Code civil. Notons cependant que le juge a sursis à statuer sur la suite à donner aux intérêts civils.

[1019] Cass. (2e ch.), 4 novembre 2020, R.G. n° P.20.1073.F, www.cass.be.

[1020] Cour eur. D.H. (4e sect.), arrêt *Bivolaru c. Roumanie* (n° 1), 28 février 2017, req. n° 28796/04.

la Cour[1021] car il estime que la violation subsiste, malgré le constat de l'atteinte à l'article 8 de la Convention européenne des droits de l'homme par le tribunal départemental de Bucarest[1022].

La Cour rappelle que le redressement d'une violation alléguée de la Convention revient aux autorités nationales. La Cour doit, pour sa part, vérifier s'il y a eu reconnaissance par les autorités nationales d'une violation d'un droit protégé par la Convention et si le redressement offert peut être considéré comme approprié et suffisant[1023]. Dans le cas d'espèce, la reconnaissance a été opérée par le tribunal départemental de Bucarest, saisi par le requérant dans le cadre d'une action en responsabilité civile délictuelle[1024]. Concernant le redressement, le tribunal a octroyé la somme symbolique de 1 RON au titre de dommage moral. La Cour estime que ce redressement est approprié et suffisant car le tribunal roumain a suivi la jurisprudence pertinente de la Cour en la matière[1025], dans laquelle elle considère que cette réparation symbolique est appropriée et suffisante[1026].

c. Respect du droit à un procès équitable

320. Impossibilité de vérifier la réalité et de contredire les éléments ayant motivé des écoutes téléphoniques. La Cour européenne des droits de l'homme se prononce dans son arrêt *Paci contre Belgique*[1027] sur le respect du droit à un procès équitable dans le cadre de la non-divulgation des ordonnances d'écoutes téléphoniques à la défense.

Dans le cas d'espèce, le requérant a été condamné pour des faits de trafic international d'armes (dossier dit « armes »). Parmi les pièces soumises aux juridictions de jugement, figuraient des copies d'ordonnances d'écoutes téléphoniques dans un autre dossier le concernant (dossier dit « voitures »). Le Ministère public a refusé de joindre la copie intégrale du dossier « voitures », privant le requérant, selon lui, du « bénéfice d'une vérification *in concreto* par les juridictions de jugement de la régularité des mesures d'écoute décidées dans ce dossier "voitures" »[1028].

La Cour rappelle qu'un procès équitable doit revêtir un caractère contradictoire impliquant, pour l'accusation comme pour la défense, la faculté de prendre connaissance des observations ou éléments de preuve produits par l'autre partie et de les discuter, ainsi que la communication à la défense de toutes les preuves pertinentes en leur possession, à charge comme à décharge[1029]. Ce droit de divulgation n'est cependant pas absolu, la Cour énonce trois conditions pour qu'une dissimulation des preuves n'altère pas le caractère équitable de la procédure : la légitimité de la non-divulgation, la compensation de la limitation des droits de la défense par la procédure suivie devant les autorités judiciaires et l'analyse de l'impact des éléments divulgués sur la solidité de la condamnation[1030].

1021 Cour eur. D.H. (4e sect.), arrêt *Bivolaru c. Roumanie* (n° 2),2 octobre 2018, req. n° 66580/12.
1022 *Ibid.*, § 165.
1023 *Ibid.*, § 168.
1024 *Ibid.*, § 169.
1025 *Ibid.*, § 172.
1026 *Ibid.*, § 173.
1027 Cour eur. D.H. (2e sect.), arrêt *Paci c. Belgique*, 17 avril 2018, req. n° 45597/09.
1028 *Ibid.*, § 88.
1029 *Ibid.*, § 84.
1030 *Ibid.*, §§ 85-87.

Dans le cas d'espèce, la Cour estime que la non-divulgation est absolument nécessaire car certains éléments devaient rester confidentiels pour mener à bien l'instruction dans le deuxième dossier (dossier « voitures »)[1031]. Ensuite, bien que la décision de non-divulgation ait été prise par le ministère public, ce qui constitue en soi une limitation des droits de la défense[1032], le reste de la procédure compense suffisamment cette limitation des droits de la défense (accès du requérant à l'ensemble du dossier répressif, écoutes ordonnées par un juge d'instruction et contrôle par les juridictions de jugement)[1033]. Enfin, la Cour constate que la condamnation ne repose pas sur les seules écoutes téléphoniques, le requérant étant notamment partiellement en aveu[1034].

321. Destruction des enregistrements de conversations téléphoniques. La Cour européenne des droits de l'homme se prononce, dans son arrêt *Samoylov*[1035], sur le caractère équitable d'une procédure pénale au cours de laquelle des enregistrements de conversations téléphoniques ont été détruits, alors qu'ils auraient pu jouer en faveur du requérant.

Après avoir rappelé l'obligation pour les autorités de poursuite, en vertu du droit au procès équitable protégé par l'article 6 de la Convention européenne des droits de l'homme, de « communiquer à la défense toutes les preuves pertinentes en leur possession, à charge comme à décharge »[1036], la juridiction strasbourgeoise conclut que le moyen est mal fondé pour deux raisons principales. Tout d'abord, la Cour considère que le fait de ne pas avoir accès aux enregistrements n'a pas été préjudiciable pour le requérant en raison, notamment, du fait qu'il a eu l'occasion d'interroger un des témoins dont la conversation fut détruite et que ce témoignage se retrouvait dans les conclusions du rapport d'expertise[1037]. Ensuite, l'illégalité de la destruction des enregistrements n'a été évoquée ni devant la cour régionale ni devant la Cour suprême russe. La Cour estime que le requérant aurait alors pu motiver spécifiquement sa demande à cet égard[1038].

2. Saisie de données électroniques

322. Saisie de fichiers numériques d'un avocat. Dans son arrêt *Kirkdök et autres contre Turquie*[1039], la Cour rappelle que les saisies opérées dans les bureaux ou les cabinets des avocats s'analysent en une ingérence dans le droit au respect du domicile et de la correspondance consacré à l'article 8 de la Convention. Sont visés, par la notion de « correspondance », les disques durs informatiques et les données électroniques, fichiers informatiques et messageries[1040]. Dans le cas d'espèce, la Cour conclut que le seul fait de retenir une copie des données électroniques saisies dans le cabinet d'avocats des requérants constitue une ingérence, même si lesdites données n'ont pas été déchiffrées, transcrites et officiellement attribuées aux requérants[1041]. Comme toutes les ingérences dans le droit au respect de la correspondance, il convient de vérifier que celle-ci est

1031 *Ibid.*, § 91.
1032 *Ibid.*, § 94.
1033 *Ibid.*, §§ 92, 93 et 95.
1034 *Ibid.*, § 97.
1035 Cour eur. D.H. (3e sect.), arrêt *Samoylov c. Russie*, 3 juillet 2018, req. no 17512/08.
1036 *Ibid.*, § 47 et Cour eur. D.H., arrêt *Wesenbeeck c. Belgique*, 23 mai 2017, req. nos 67496/10 et 52936/12, § 67.
1037 Cour eur. D.H. (3e sect.), arrêt *Samoylov c. Russie*, 3 juillet 2018, req. no 17512/08, § 48.
1038 *Ibid.*, § 48 et Cour eur. D.H., arrêt *Bendenoun c. France*, 24 février 1994, §52.
1039 Cour eur. D.H. (2e sect.), arrêt *Kirkdök et autres c. Turquie*,3 décembre 2019, req. no 14704/12.
1040 *Ibid.*, § 34.
1041 *Ibid.*, § 36.

prévue par la loi, poursuit un but légitime et est nécessaire dans une société démocratique. Dans ce cas, la Cour estime que « les mesures imposées aux requérants quant à la saisie de leurs données électroniques et au refus de les restituer ou de les détruire n'ont répondu à aucun besoin social impérieux, qu'elles n'étaient pas, en tout état de cause, proportionnées aux buts légitimes visés et que, de ce fait, elles n'étaient pas nécessaires dans une société démocratique »[1042].

3. Recherche dans un système informatique et sur Internet

323. Recherche dans un système informatique et secret professionnel des médecins et des avocats. Dans un arrêt du 6 décembre 2018[1043], la Cour constitutionnelle annule l'article 39*bis*, § 3, du Code d'instruction criminelle, ainsi que l'entièreté des modifications apportées à l'article 39*bis* du code précité par l'article 2 de la loi du 25 décembre 2016[1044].

Tout d'abord, la Cour rappelle que l'extension de la recherche dans un système informatique ou une partie de celui-ci, entamée dans un système informatique qui a été saisi ou qui peut être saisi par le procureur du Roi, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée implique une ingérence grave dans le droit au respect de la vie privée. Par conséquent, une telle extension doit être autorisée dans les mêmes conditions que la perquisition et demeurer de la compétence du juge d'instruction et non du procureur du Roi[1045]. Le paragraphe 3 de l'article 39*bis*, en ce qu'il attribue cette compétence au procureur Roi, doit dès lors être annulé.

Ensuite, l'article 39*bis* du Code d'instruction criminelle ne prévoit pas de garanties spécifiques pour les recherches non secrètes dans le système informatique d'un avocat ou d'un médecin alors que de telles garanties sont prévues pour les recherches secrètes visées à l'article 90*octies* du même code. Selon la haute juridiction, « il n'est pas justifié que la clause de protection du secret professionnel des avocats et des médecins ne soit prévue que lorsque la recherche dans un système informatique qu'ils utilisent à titre professionnel est menée en secret et non lorsqu'elle est portée à leur connaissance. En effet, l'ingérence dans le droit au respect de la vie privée des personnes qui leur ont confié des informations couvertes par leur secret professionnel intervient de la même manière, que la recherche soit menée à l'insu ou non de l'avocat ou du médecin concerné »[1046]. L'article 39*bis* du Code d'instruction criminelle, tel que modifié par la loi du 25 décembre 2016, est

1042 *Ibid.*, § 58.

1043 C.C., arrêt n° 174/2018 du 6 décembre 2018, *M.B.* (1re éd.), 22 janvier 2019 (extrait), p. 7686 ; *Computerr.*, 2019, p. 134, note W. Yperman et F. Verbruggen, « Wetgever én Grondwettelijk Hof in de knoop met criteria voor regulering IT-speurwerk » ; *N.j.W.*, 2019, p. 201, note S. Royer, « Wet 25 december 2016 digitaal speurwerk op twee punten vernietigd » ; *N. C.*, 2019, p. 436 ; *Rev. dr. pén.*, 2019, p. 684, note ; *R.W.*, 2018-2019 (sommaire), p. 1159 ; *T. Strafr.*, 2019, p. 243, note C. Conings, « Grondwettelijk Hof buigt zich over de wet digitale recherche » ; *T.V.W.*, 2019, p. 40. Voy. également P. Monville, M. Giacometti et L. Grisard, « La collecte des preuves numériques en droit belge après l'arrêt de la Cour constitutionnelle du 6 décembre 2018 », *Rev. dr. pén.*, 2019, pp. 993-1032.

1044 Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017, p. 2738.

1045 C.C., arrêt n° 174/2018, 6 décembre 2018, B.16.4.

1046 C.C., arrêt n° 174/2018, 6 décembre 2018, B.26.1.

par conséquent annulé en ce qu'il ne prévoit pas de disposition spécifique en vue de protéger le secret professionnel des médecins et des avocats.

4. Obtention de renseignements associés à une adresse IP dynamique

324. Utilisation de l'adresse IP dynamique par les services de police et anonymat sur Internet. Dans son arrêt *Benedik c. Slovénie*[1047], la Cour européenne des droits de l'homme se prononce sur l'utilisation d'adresses IP d'internautes par la police slovène dans le cadre de partage de contenus à caractère pédopornographique. En l'espèce, les fichiers contenant des contenus illégaux étaient échangés via un réseau de partage de fichiers en *peer-to-peer* dans lequel chacun des ordinateurs connectés faisait office à la fois de client et de serveur. Ainsi, chaque utilisateur pouvait accéder à tous les fichiers mis à disposition pour le partage par d'autres utilisateurs du réseau et les télécharger pour son usage personnel. Les adresses IP dynamiques[1048] des utilisateurs du réseau ont été collectées par la police suisse, puis transmises à la police slovène. Cette dernière a obtenu d'un fournisseur d'accès Internet le nom et l'adresse de l'un de ses abonnés, qui était associé à l'une des adresses IP dynamiques en question. Le contrat de fourniture d'accès à Internet était, en l'occurrence, conclu au nom du père du requérant[1049]. Il incombe à la Cour de déterminer si le requérant, ou tout autre individu utilisant Internet, pouvait raisonnablement s'attendre à ce que son activité en ligne soit anonyme.

Après avoir déterminé l'applicabilité de l'article 8 de la Convention européenne des droits de l'homme – notamment en raison du fait que l'obtention des informations relatives aux abonnés avait pour seul but d'identifier une personne particulière à l'origine du contenu téléchargé[1050] – la Cour reconnait la qualité de victime au requérant en raison du suivi de ses activités sur le réseau Internet. Aux yeux de la Cour, le fait que le nom et le prénom de l'abonné renvoient à l'identité du père du requérant n'a aucun effet sur ses attentes légitimes quant au respect de sa vie privée[1051].

La Cour rappelle sa jurisprudence antérieure – notamment l'arrêt *Delfi*[1052] – dans laquelle elle reconnait des degrés variables d'anonymat sur Internet. Tenant compte des circonstances

1047 Cour eur. D.H., arrêt *Benedik c. Slovénie*, 24 avril 2018, req. n° 62357/14. Pour un commentaire, voy. not. J. Herveg et J.-M. Van Gyseghem, « La protection des données à caractère personnel en droit européen-Chronique de jurisprudence (2018), *J.E.D.H.*, 2019/1, pp. 45 et s.

1048 En son § 96, la Cour rappelle que : « Une adresse IP est un numéro unique attribué à chaque dispositif d'un réseau, qui permet aux dispositifs de communiquer entre eux. Contrairement à l'adresse IP statique, qui est attribuée de manière permanente à une interface réseau particulière d'un dispositif particulier, une adresse IP dynamique est attribuée à un dispositif par le FAI de manière temporaire, généralement à chaque fois que le dispositif se connecte à Internet » (traduction libre).

1049 Cour eur. D.H., arrêt *Benedik c. Slovénie*, 24 avril 2018, req. n° 62357/14, §§ 6 et s.

1050 *Ibid.*, §§ 100 et s.

1051 *Ibid.*, §§ 111 et s. De surcroît, en son paragraphe 103, la Cour insiste sur l'importance d'une interprétation large de la notion de vie privée, permettant aux individus d'invoquer leur droit à la vie privée à l'égard de données qui, bien que neutres, sont collectées, traitées et diffusées collectivement et sous une forme ou d'une manière telle que leurs droits au titre de l'article 8 de la Convention peuvent être invoqués.

1052 Cour eur. D.H. (gde ch.), arrêt *Delfi AS c. Estonie*, 16 juin 2015, req. n° 64569/09. Pour un commentaire, voy. not. P. Ombelet et P. Valcke, « Geen aansprakelijkheid van de uitgever die een nieuwsportaal op internet uitgeeft voor beledigingen gepost door anonieme derden », *A&M*, 2015, liv. 5-6, pp. 417-422 ; K. Lemmens, « Condamnation à des dommages-intérêts d'une société éditant un portail d'actualités sur internet. Je suis anonyme. Qui est juridiquement responsable de mes dires? », *R.D.T.I.*, 2015, liv. 61, pp. 127-138 ; E. Montero et Q. Van Enis, « Les gestionnaires de forums et portails d'actualités cueillis à froid par la Cour de Strasbourg », *Rev. trim. dr. h.*, 2017, pp. 953-981. Voy. aussi Q. Van Enis,

concrètes de l'espèce, la Cour admet que le requérant pouvait légitimement s'attendre à un degré élevé d'anonymat pour ses activités en ligne[1053].

En conséquence, la Cour doit déterminer si l'atteinte au respect de la vie privée respecte bien les garanties imposées au second paragraphe de l'article 8 de la Convention européenne des droits de l'homme. Pour qu'une faute dans le chef d'un État membre soit retenue, il faut notamment démontrer l'absence de garanties adéquates et effectives contre les abus. Cette appréciation dépend de toutes les circonstances de l'espèce, telles que la nature, la portée et la durée des mesures éventuelles, les motifs requis pour les ordonner, les autorités compétentes pour les autoriser, les exécuter et les contrôler, ainsi que le type de recours prévu par le droit national[1054]. Considérant que la mesure contestée, à savoir l'obtention par la police des informations relatives à l'abonné associé à l'adresse IP dynamique sans intervention d'un juge, manque de clarté et n'offre pas de garanties suffisantes contre une ingérence arbitraire dans les droits de l'article 8, la Cour considère que l'ingérence n'est pas « prévue par la loi », condition pourtant essentielle pour porter valablement atteinte à un droit fondamental[1055].

5. Géolocalisation comme technique de surveillance policière

325. Géolocalisation et surveillance policière. Dans son arrêt *Ben Faiza contre France*[1056], la Cour européenne des droits de l'homme s'interroge sur l'utilisation de la technologie de géolocalisation en matière de surveillance policière. En substance, l'affaire concerne le démantèlement d'un trafic de stupéfiants. Après l'interception de communications téléphoniques, ordonnée par le juge d'instruction, celui-ci a donné son autorisation aux services de police pour l'installation d'un dispositif de localisation des véhicules identifiés comme servant au trafic. L'enquête a abouti en 2010[1057]. Dans un arrêt de 2010[1058], la Cour avait déjà jugé que la mise en place d'un dispositif de surveillance via GPS constitue une ingérence dans le droit à la vie privée consacré par l'article 8 de la Convention. Le constat est ici renforcé dès l'instant où la mesure de géolocalisation examinée est associée à la mise en place d'un dispositif technique permettant de capter et d'enregistrer les conversations des personnes se trouvant dans le véhicule[1059]. Le débat s'est cristallisé autour de la condition de légalité, qui nécessite de vérifier que « la mesure incriminée ait une base légale en droit interne. Pour juger de l'existence d'une telle "base légale", il y a lieu de prendre

« Droit des médias, liberté d'expression et nouvelles technologies – Chronique de jurisprudence 2012-2014 », *R.D.T.I.*, 2015, pp. 163-164, n^{os} 289-293. Sur le droit à l'anonymat sur Internet, voy. not. F. Tréguer, « Anonymat et chiffrement, composantes essentielles de la liberté de communication », in *L'Europe des droits de l'homme à l'heure d'Internet* (C. de Terwangne et Q. Van Enis, dir.), Bruxelles, Bruylant, 2019, pp. 265-292.

1053 La Cour européenne des droits de l'homme réfute ainsi l'argument de la Cour constitutionnelle slovène selon lequel le requérant, en n'ayant pas dissimulé son adresse IP dynamique ne pouvait légitimement pas s'attendre à la protection de sa vie privée sur Internet ; Cour eur. D.H., arrêt *Benedik c. Slovénie*, 24 avril 2018, req. n° 62357/14, points 116 et s.

1054 *Ibid.*, § 125.

1055 *Ibid.*, §§ 126 et s.

1056 Cour eur. D.H., arrêt *Ben Faiza c. France*, 8 février 2018, req. n° 31446/12, note K. Keyaerts et F. Verspeelt, « Geolocatiesurveillance Tijdens eens strafonderzoek », *Politie & Recht*, 2019/3, p. 123.

1057 Cour eur. D.H., arrêt *Ben Faiza c. France,* 8 février 2018, req. n° 31446/12, §§ 5 et s.

1058 Cour eur. D.H., arrêt *Uzun c. Allemagne*, 2 décembre 2010, req. n° 35623/05.

1059 Cour eur. D.H., arrêt *Ben Faiza c. France*, 8 février 2018, req. n° 31446/12, §§ 53 et 54.

en compte non seulement les textes législatifs pertinents, mais aussi la jurisprudence »[1060]. En l'occurrence, le caractère imprécis de la disposition de droit français sur la base de laquelle les autorités nationales ont accordé l'apposition d'un dispositif GPS dans le véhicule ne permet pas de reconnaître la validité de ladite base légale en droit interne[1061]. En poursuivant son analyse, la Cour est d'avis qu'une telle imprévisibilité ne pouvait pas, au moment des faits, être compensée par la jurisprudence nationale[1062]. Elle souligne également l'absence de « garanties adéquates et suffisantes contre le risque d'abus inhérent à tout système de surveillance secrète »[1063].

6. Accès à une banque de données par les services de police

326. Dispense d'autorisation pour accéder à des données à caractère personnel par les services de police. La loi du 14 juin 2017 modifiant l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[1064] a fait l'objet de deux recours en annulation devant la Cour constitutionnelle[1065]. Cette dernière statue par un arrêt du 8 novembre 2018[1066].

Le troisième alinéa de l'article 36*bis* de la loi du 8 décembre 1992 énonce que toute communication électronique de données à caractère personnel par un service public fédéral ou par un organisme public doté de la personnalité juridique qui relève de l'autorité fédérale requiert une autorisation de principe, en règle générale de la part du comité sectoriel pour l'autorité fédérale. Cette autorisation de principe n'est pas requise lorsque la communication est déjà soumise à une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée et dans les cas fixés par le Roi.

Le nouvel alinéa vise à dispenser les services de police, tels que définis à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux, de toute autorisation préalable du comité sectoriel dans l'exercice de leurs missions de police administrative et de police judiciaire. Une telle dérogation résultait déjà de l'article 1er de l'arrêté royal du 4 juin 2003 « fixant dérogation à l'autorisation visée à l'article 36*bis* de la loi du 8 décembre 1992 relative à la

1060 *Ibid.*, § 56.

1061 *Ibid.*, §§ 58 et s.

1062 En effet, les mesures de surveillance policière ont été ordonnées en 2009 et 2010. Or, le premier arrêt de la Cour de cassation française se prononçant sur la légalité de la géolocalisation au cours d'une information judiciaire n'a été rendu qu'en 2011. Ce constat est renforcé par l'adoption d'une loi datant du 28 mars 2014, par laquelle la France encadre le recours à la géolocalisation et renforce la protection du droit au respect de la vie privée ; Cour eur. D.H., arrêt *Ben Faiza c. France*, 8 février 2018, req. n° 31446/12, §§ 58-61.

1063 *Ibid.*, § 59. Notons qu'en revanche, dans le même arrêt, la Cour européenne des droits de l'homme a validé la collecte d'informations concernant la date, la durée des appels téléphoniques et les numéros composés. Si une telle mesure porte bien atteinte au droit à la vie privée, la Cour reconnaît que l'ingérence était prévue par le droit français, qu'elle poursuivait un but légitime – à savoir la lutte contre le trafic de stupéfiants et le blanchiment – et que ladite ingérence était nécessaire dans une société démocratique (*Ibid.*, §§ 66 et s.).

1064 Si besoin est, rappelons que cette loi a été abrogée, suite à l'adoption du RGPD, et remplacée par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*M.B.*, 5 septembre 2018).

1065 Notons que l'article 36*bis* de la loi du 8 décembre 1992 a été abrogé par la loi du 3 décembre 2017 portant création de l'Autorité de protection des données avec effet au 25 mai 2018, ce qui correspond à l'entrée en application du RGPD. Ceci étant, la Cour constitutionnelle note que l'article 36*bis* a produit des effets jusqu'au 24 mai 2018, de sorte que les recours en annulation ne sont pas devenus sans objet.

1066 C.C., arrêt n° 153/2018, 8 novembre 2018.

protection de la vie privée à l'égard des traitements de données à caractère personnel au profit de la banque de données nationale générale de la police intégrée structurée à deux niveaux». Elle était justifiée au regard du cadre légal détaillé encadrant la fonction de police, à savoir la loi du 5 août 1992 sur la fonction de police. Une telle dérogation n'était néanmoins pas applicable à la consultation des données à caractère personnel contenues dans la Banque-Carrefour des véhicules, la Cour de cassation ayant jugé, sur pied de l'article 18 de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules et l'arrêté royal du 8 juillet 2013 portant exécution de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules, qu'une autorisation du Comité sectoriel est requise pour tout accès aux données à caractère personnel de la Banque-Carrefour des véhicules, en ce compris de la part des services de police[1067].

Cette situation menait à une incertitude juridique qu'il convenait de gommer par voie législative. Tel est l'objectif de la loi du 14 juin 2017 présentement attaquée.

327. Droit au respect de la vie privée. Dans la première branche du moyen, les parties requérantes font valoir que le dernier alinéa de l'article 36*bis* de la loi du 8 décembre 1992, tel qu'il a été inséré par l'article 2 de la loi attaquée, viole le droit au respect de la vie privée et dès lors que la police se voit conférer un accès général aux banques de données des services publics fédéraux et des organismes publics fédéraux sans que cet accès soit assorti de garanties visant à protéger le droit au respect de la vie privée.

La Cour constitutionnelle observe que le fait de dispenser les services de police de l'autorisation préalable n'a nullement pour effet de les dispenser du respect de la loi du 8 août 1992, dont les principes sont repris dans la loi du 5 août 1992 sur la fonction de police. En particulier, il découle de cette dernière loi que toutes les informations et données à caractère personnel qui sont traitées par les services de police peuvent être contrôlées par l'Organe de contrôle (article 44/1) et que toutes les banques de données policières relèvent du pouvoir de contrôle de cet organe (article 44/2). En outre, chaque zone de police et le commissariat général, chaque directeur général et chaque direction de la police fédérale traitant des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques données visées à l'article 44/2, §§ 1er et 3 est tenu, en vertu de l'article 44/3, § 1er, alinéa 3, de la loi du 5 août 1992 de désigner un conseiller en sécurité et en protection de la vie privée. Par ailleurs, les services de police sont également soumis au contrôle du Comité permanent de contrôle des services de police (Comité permanent P)[1068].

À la lumière de ces considérations, le législateur a pu estimer qu'il existait déjà des garanties législatives suffisantes pour prévenir les abus et que partant, il n'était pas nécessaire de soumettre la communication de données à caractère personnel aux services de police par un service ou organisme public fédéral ou l'accès des services de police aux banques de données d'un tel service ou

1067 Cass., 13 décembre 2016, R.G. n° P.16.0682.N. Pour un commentaire, voy. not. E. Degrave, «PV pour excès de vitesse: les services de police peuvent-ils accéder librement aux données de la DIV?», *R.D.T.I.*, 2016, n° 65, pp. 63-71. Voy. aussi C. Fievet, L. Gérard, N. Gillart, e.a., «Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information – Chronique de jurisprudence 2015-2017», *R.D.T.I.*, 2017/3, p. 161, n° 211.

1068 Article 1er de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

organisme public à une autorisation préalable du Comité sectoriel. La Cour conclut donc que le premier moyen, en sa première branche, n'est pas fondé[1069].

328. Principe de légalité en matière pénale. Dans la deuxième branche du premier moyen, « les parties requérantes font valoir que l'article 36*bis*, dernier alinéa, de la loi du 8 décembre 1992, tel qu'il a été inséré par l'article 2 de la loi attaquée, est contraire au principe de la légalité en matière pénale, tel qu'il est garanti par l'article 12, alinéa 2, de la Constitution, en ce que, lorsque l'exercice d'un pouvoir d'investigation constitue une ingérence dans le droit au respect de la vie privée, les conditions relatives à cette ingérence doivent être prévues par la loi, ce qui ne serait pas le cas en l'espèce »[1070].

La Cour rappelle ici les considérations émises plus haut d'après lesquelles l'ingérence dans le droit au respect de la vie privée discutée est entourée de garanties législatives suffisantes pour éviter les abus. Pour autant, il faut observer que les garanties mises en place sous l'angle du droit à la vie privée ne sont pas nécessairement comparables à celles instaurées sous l'angle du principe de légalité pénale. À cet égard, on notera que la Cour européenne des droits de l'homme veille à distinguer les garanties applicables en fonction du droit fondamental en cause. Elle est ainsi plus exigeante s'agissant des garanties à mettre en place en vertu de l'article 6 de la Convention que celles à prévoir en vertu de l'article 8[1071].

7. Blocage d'un site Internet contraire à l'ordre public et aux bonnes mœurs

329. Absence d'information préalable en cas de blocage d'un site Internet. Si des données informatiques forment l'objet de l'infraction ou ont été produites par une infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi peut rendre ces données inaccessibles ou, après en avoir pris copie, les retirer conformément à l'article 39*bis*, § 6, du Code d'instruction criminelle. Il s'agit d'une mesure conservatoire. Le procureur du Roi peut, dans le respect de l'article 28*sexies*, § 3, du Code d'instruction criminelle, prononcer le maintien du blocage du site Internet lorsque la levée de l'acte présente un danger pour les personnes ou les biens, ou dans les cas où la loi prévoit la restitution ou la confiscation desdits biens. Le juge du fond pourra ensuite prononcer la « confiscation » du site Internet dès lors que les données du site Internet données forment l'objet d'une infraction en vertu de l'article 42, 1°, du Code pénal. Dans un tel cas, la confiscation prendra la forme d'un blocage du site Internet.

S'il découle de l'article 39*bis*, § 7, du Code d'instruction criminelle que les autorités judiciaires doivent avertir le « responsable du système informatique » lorsque ledit système a fait l'objet d'une recherche[1072], la cour d'appel de Bruxelles a toutefois décidé, dans un arrêt du 9 mai 2018, qu'une telle information n'était pas requise dans le cas où l'accès à un site Internet – en l'occurrence, le site Internet www.RichMeetBeautiful.com – a été bloqué en application de l'article 39*bis*,

1069 C.C., arrêt n° 153/2018, 8 novembre 2018, B.14.
1070 *Ibid.*, B.15.
1071 En ce sens, voy. A. Lachapelle, « Le respect du droit à la vie privée dans les traitements d'informations à des fins fiscales : état des lieux de la jurisprudence européenne (2e partie) », *R.G.F.C.P.*, n° 2016/10, p. 55.
1072 Voy. C.C., arrêt n° 174/2018, 6 décembre 2018, B.18.1 à B.23.

§ 6, du Code d'instruction criminelle[1073]. Ce faisant, il convient de distinguer la recherche dans un système informatique (article 39*bis*, § 7) des mesures techniques visant à rendre des données informatiques inaccessibles (article 39*bis*, § 6)[1074].

C. Obligations de collaboration dans l'environnement numérique

1. Obligation de conservation de données

330. Obligation générale de conservation des données dans le secteur des communications électroniques. Quatre recours en annulation ont été portés devant la Cour constitutionnelle à propos de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques[1075].

La loi attaquée entend répondre à l'annulation, par l'arrêt de la Cour constitutionnelle n° 84/2015 du 11 juin 2015[1076], de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques[1077]. L'arrêt de la Cour constitutionnelle fait suite à l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire « *Digital Rights Ireland* »[1078] qui tend à invalider la directive 2006/24/CE dite « conservation des données ».

En substance, les requérants estiment qu'en érigeant une obligation généralisée et indifférenciée pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, la loi attaquée est contraire au droit à la sécurité, au droit à la vie privée et au droit au respect des données à caractère personnel.

La Cour a décidé de poser trois questions préjudicielles à la Cour de justice de l'Union européenne. Celle-ci a rendu son arrêt en date du 6 octobre 2020 dans un arrêt dit « Quadrature du Net » commenté dans la partie « Vie privée » de la présente chronique.

331. Obligation de conservation des données à caractère personnel des utilisateurs de cartes SIM prépayées par les opérateurs de téléphonie mobile à des fins de protection de la sécurité nationale. Dans un arrêt phare du 30 janvier 2020, la Cour européenne des droits de l'homme s'est prononcée sur la conformité avec l'article 8 de la Convention européenne des droits de l'homme de la loi allemande sur les télécommunications de 2004 en ce qu'elle prévoit une obligation légale pour les opérateurs de téléphonie mobile de recueillir des données person-

1073 Bruxelles (mise acc.), 9 mai 2018.

1074 Une telle obligation n'est, certes, pas prescrite à peine de nullité. Néanmoins, on peut se demander si l'absence d'information dans un tel cas de figure n'est pas susceptible de compromettre l'exercice du droit à un procès équitable et donc d'être sanctionnée sur pied de l'article 32, troisième tiret, du titre préliminaire du Code de procédure pénale, qui implémente les enseignements de la jurisprudence « Antigone ».

1075 C.C., arrêt n° 96/2018, 19 juillet 2018.

1076 Pour un commentaire de cet arrêt, voy. not. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, p. 208, n° 289.

1077 *Doc.*, Ch., 2015-2016, n° 54-1567/001, p. 4.

1078 C.J.U.E. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, 8 avril 2014, C-293/12 et C-594/12, ECLI:EU:C:2014:238. Pour un commentaire de cet arrêt, voy. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, pp. 208-207, n° 288.

nelles des utilisateurs de cartes SIM prépayées et de les tenir à la disposition des autorités[1079]. Ces dernières peuvent demander à se voir transmettre les données (nom, adresse et date de naissance) en l'absence de toute décision de justice et sans devoir le notifier préalablement aux personnes concernées.

Par six voix contre une, la Cour (cinquième section) a cependant conclu à l'absence de violation de l'article 8 de la Convention[1080]. Elle a été attentive à l'absence de consensus européen quant à la collecte et à la conservation d'informations sur les détenteurs de cartes SIM prépayées. Il s'ensuit que les État membres du Conseil de l'Europe, parmi lesquels l'Allemagne, jouissent d'une ample marge d'appréciation[1081]. Celle-ci est d'autant plus grande que la sécurité nationale est en jeu. Si les État membres apprécient librement le *type* de système d'interception permettant de sauvegarder au mieux la sécurité nationale, la Cour contrôle néanmoins la *mise en œuvre* du système d'interception sélectionné[1082]. La Cour rappelle, à la suite de son arrêt *Leander c. Suède*[1083], que la simple obligation de conserver des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la Convention européenne des droits de l'homme[1084]. L'obligation de conservation de ces données repose, en l'occurrence, sur une base en droit interne, la section 11 de la loi allemande sur les télécommunications[1085], et poursuit des finalités légitimes de sécurité publique, de prévention des troubles ou de la criminalité et de protection des droits et libertés d'autrui[1086]. L'obligation de conservation est, ensuite, nécessaire dans une société démocratique étant entendu qu'il convient d'adapter les moyens d'investigation des autorités répressives et des agences de sécurité à l'évolution des moyens de télécommunication et des comportements en matière de communication[1087]. La Cour relève également que les données enregistrées, sans être insignifiantes, ne sont pas comparables aux données visées par les obligations de conservation examinées par la Cour de justice de l'Union européenne dans le cadre des célèbres affaires « *Digital Rights Ireland* »[1088] et « *Tele2* »[1089]. En outre, la loi allemande prévoit des garanties adéquates et suffisantes de sorte qu'un juste équilibre est ménagé entre les intérêts privés et les intérêts publics[1090]. Conformément aux règles européennes de protection des données, la transmission de données aux autorités (extraction) se limite, par ailleurs, aux données

1079 Cour eur. D.H. (5e sect.), arrêt *Breyer c. Allemagne*, 30 janvier 2020, req. n° 50001/12.

1080 Les requérants invoquaient également une violation de l'article 10 de la CEDH, mais la Cour a considéré que les griefs des requérants résidaient principalement dans l'obligation de conservation de données personnelles sous l'angle du droit à la vie privée (§ 61).

1081 Cour eur. D.H. (5e sect.), arrêt *Breyer c. Allemagne*, 30 janvier 2020, req. n° 50001/12, § 80.

1082 Sur cette jurisprudence, voy. *infra*, n° 337.

1083 Cour eur. D.H., arrêt *Leander c. Suède*, 26 mars 1987, req. n° 9248/81, § 48.

1084 Cour eur. D.H. (5e sect.), arrêt *Breyer c. Allemagne*, 30 janvier 2020, req. n° 50001/12, § 81.

1085 *Ibid.*, §§ 84-85.

1086 *Ibid.*, §§ 84-87.

1087 *Ibid.*, § 88.

1088 C.J.U.E. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, 8 avril 2014, C-293/12 et C-594/12, EU:C:2014:238. Pour un commentaire, voy. not. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, pp. 207-208, n° 288.

1089 C.J.U.E. (gde ch.), arrêt *Tele2 Sverige AB c. Post- och telestyrelsen et Secretary of State for the Home Department c. Tom Watson e.a.*, 21 décembre 2016, C-203/15 et C-698/15, EU:C:2016:970. Pour un commentaire, voy. not. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, p. 209, n° 291.

1090 La durée de conservation est, par exemple, limitée – année civile qui suit l'année où la relation contractuelle a pris fin – et cette durée ne paraît pas excessive. Des garanties encadrent par ailleurs les possibilités de consultation et

nécessaires (§ 100). Aussi, si la demande d'extraction ne doit pas être précédée par une information de la personne concernée, d'autres mesures de contrôle sont prévues, *a priori* et *a posteriori*, dans le respect des règles européennes de protection des données (§§ 102-103).

2. Obligation de communication de données

a. Obligation de communication dans le cadre d'une enquête pénale

332. Obligation de collaboration des fournisseurs étrangers de services de messagerie électronique. Dans un arrêt du 19 février 2019[1091], la Cour de cassation précise la portée des articles 88*bis* et 90*quater*, § 2, du Code d'instruction criminelle. L'affaire en cause concernait l'entreprise de messageries Internet *Skype Communications*[1092]. Depuis 2012, il était demandé à cette dernière de collaborer à une enquête pénale – communication de données de trafic et interception de communications – à l'encontre d'un de ses utilisateurs, qui utilisait la messagerie *Skype* afin de communiquer avec ses complices[1093]. Celle-ci s'opposait néanmoins, se retranchant derrière son siège social établi au Grand-Duché de Luxembourg. En l'absence d'une présence physique en Belgique, les autorités belges sont, selon elle, tenues de suivre les procédures d'entraide judiciaires et de s'adresser aux autorités luxembourgeoises[1094].

D'après la haute juridiction judiciaire, les articles 88*bis* et 90*quater*, § 2, du Code d'instruction criminelle « permettent au juge d'instruction belge, dans le cadre de son instruction, de demander à chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de messagerie électronique dont l'activité économique s'adresse activement aux consommateurs en Belgique, de communiquer les informations ou de fournir l'assistance technique visées en l'espèce, indépendamment du lieu où cet opérateur ou ce fournisseur est établi ou du lieu où se situe l'infrastructure requise pour donner suite à la demande du juge d'instruction »[1095].

La Cour de cassation prolonge ainsi les enseignements de l'affaire « *Yahoo !* »[1096], rappelant, d'une part, qu'« un tel opérateur ou fournisseur est soumis à la législation belge du seul fait de sa parti-

d'utilisation futures des données conservées. La loi allemande permet du reste de déterminer avec précision les autorités habilitées à demander des informations.

1091 Cass., 19 février 2019, R.G. n° P.17.1229.N.

1092 Pour un commentaire de l'arrêt de la Cour de cassation et un résumé de l'affaire « *Skype* », voy. V. Franssen et M. Corhay, « La fin de la saga Skype : les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger », *R.D.C./T.B.H.*, 2019, n° 8, pp. 1009-1022.

1093 Pour un commentaire des décisions des juridictions dans cette affaire, voy. not. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, pp. 210-211, n^{os} 294-295.

1094 L'entreprise *Skype* avançait, par ailleurs, l'impossibilité technique d'intercepter le contenu des communications, le logiciel de messagerie étant fondé une architecture *peer-to-peer*.

1095 Cass., 19 février 2019, R.G. n° P.17.1229.N, point 9.

1096 Cass., 1er décembre 2015, R.G. n° P.13.2082.N. Dans le cadre de cette affaire, la Cour de cassation a jugé que les autorités judiciaires belges peuvent directement appliquer le droit belge à tous les fournisseurs de services étrangers virtuellement présents en Belgique sans qu'une procédure d'entraide judiciaire ne soit requise. Pour une analyse, voy. not. R. Roex, « Belgische justitie kan rechtstreeks informatie opvragen van Amerikaanse techreuzen », *Juristenkrant*, 2015, n° 319, p. 5 ; K. De Schepper, « Doek valt over *Yahoo*-zaak », *Computerr.*, 2016, n° 2016/35 ; V. Franssen, « The Belgian Internet Investigatory Powers Act. A Model to Pursue at European Level? », *E.D.P.L.*, n° 2017/4, pp. 538-540. Voy. aussi C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, p. 211, n° 295. L'affaire « *Yahoo* » a été suivie par une modification du Code d'instruction criminelle et du Code pénal par une loi du 25 décembre 2016 (*M.B.*, 17 janvier 2017).

cipation active à la vie économique en Belgique. D'autre part, l'obligation de coopérer ainsi visée ne requiert pas l'intervention des autorités judiciaires belges à l'étranger. Par conséquent, le juge d'instruction n'est pas tenu d'adresser sa demande d'entraide judiciaire à l'État où le siège ou l'infrastructure de cet opérateur ou de ce fournisseur se situent et n'est pas davantage lié par la législation de ce pays »[1097].

b. Obligation de communication à des fins de prévention des infractions

333. Obligation des transporteurs et opérateurs de voyage de communiquer les données relatives aux passagers, dites données « PNR » (« *Passenger Name Record* »). Par un arrêt du 17 octobre 2019, la Cour constitutionnelle s'est prononcée sur un recours en annulation totale ou partielle de la loi du 25 décembre 2016 « relative au traitement des données des passagers », introduit par l'ASBL « Ligue des Droits de l'Homme »[1098].

La loi du 25 décembre 2016 vise à « créer un cadre légal afin d'imposer à différents secteurs de transport de personnes à caractère international (aérien, ferroviaire, routier international et maritime) et opérateurs de voyage de transmettre les données de leurs passagers à une banque de données gérée par le SPF Intérieur »[1099].

La Cour constitutionnelle juge que certaines mesures prévues par la loi du 25 décembre 2016, telle que la création d'une base de données passagers et sa gestion par une Unité d'Information des Passagers (UIP), en l'occurrence le BelPIU du Centre de crise National, sont conformes au droit à la vie privée et au droit à la protection des données à caractère personnel[1100]. Pour autant, elle s'interroge notamment sur le caractère général – liste non exhaustive de données – et indifférencié – à l'égard de toute personne que cette personne soit ou non susceptible de présenter un risque pour la sécurité publique – des obligations de traitement de données « PNR » prévues par la directive « PNR » que la loi du 25 décembre vise à transposer, au regard de ces mêmes droits. C'est pourquoi elle décide de poser dix questions préjudicielles à la Cour de justice de l'Union européenne[1101]. L'affaire (C-817/19) est actuellement pendante.

1097 Cass., 19 février 2019, P.17.1229.N, point 9.

1098 C.C., arrêt n° 135/2019, 17 octobre 2019.

1099 *Doc.*, Ch., 2015-2016, n° 54-2069/001, p. 6. Cette loi transpose trois directives européennes : la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 « relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », dite directive « PNR » (« Passenger Name Record »), la directive 2004/82/CE du Conseil du 29 avril 2004 « concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers » (« Advanced Passenger Information »), dite directive « API », et la directive 2010/65/UE du Parlement européen et du Conseil du 20 octobre 2010 « concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres et abrogeant la directive 2002/6/CE ». La première directive s'inscrit dans le cadre du renforcement de la lutte contre le terrorisme et la criminalité grave tandis que les deuxième et troisième directives visent à lutter contre l'immigration clandestine et à améliorer le contrôle aux frontières.

1100 C.C., arrêt n° 135/2019, 17 octobre 2019, B.59.2. Comme le note la Cour, la création d'une banque de données des passagers n'est pas prévue expressément par la directive « PNR » mais elle constitue un élément essentiel du système mis en place par la directive « PNR », que la loi du 25 décembre 2016 transpose.

1101 La C.J.U.E. a déjà eu à connaître d'un système « PNR » dans le cadre du projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers. Son champ d'application était néanmoins plus limité puisqu'il visait « le transfert systématique et continu des données PNR de l'ensemble des passagers aériens empruntant des vols entre l'Union et le Canada » (C.J.U.E., avis n° 1/15, 26 juillet 2017, point 127). L'avis de la C.J.U.E.

3. Obligation de coopération de l'inculpé et droit au silence

334. Collaboration de l'inculpé à la recherche dans un système informatique. Dans un arrêt du 4 février 2020[1102], la Cour de cassation se penche sur la compatibilité entre l'obligation de fournir les codes d'accès à des téléphones prévue à l'article 88*quater* du Code d'instruction criminelle et le droit au silence et de ne pas s'auto-incriminer.

L'article 88*quater*, § 3, du Code d'instruction criminelle sanctionne, entre autres, la personne, qui, bien qu'elle connaisse le code d'accès d'un système informatique tel qu'un téléphone portable à fouiller, refuse de le communiquer malgré une injonction du juge d'instruction. Cette disposition s'applique à quiconque ayant une connaissance particulière du système informatique, en ce compris l'inculpé. Elle n'est pas, selon la Cour, incompatible avec le droit de ne pas s'auto-incriminer consacré aux articles 6, § 2, de la Convention européenne des droits de l'homme, 14, §§ 2 et 3, du Pacte international relatif aux droits civils et politiques et 6 et 7 de la directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales[1103].

Néanmoins, il est nécessaire que l'appareil ait déjà été localisé au moment de l'information demandée sans recourir à la contrainte sur la personne et que l'on puisse démontrer que la personne en question connaît le code d'accès au-delà de tout doute raisonnable[1104].

335. Absence de sanction pénale en cas de refus par l'inculpé de donner accès à un système informatique et à des données. Quelques jours après la Cour de cassation, la Cour constitutionnelle se prononce également sur l'article 88*quater* du Code d'instruction criminelle à l'occasion d'une question préjudicielle posée par la cour d'appel d'Anvers[1105]. Cette dernière s'interrogeait sur la compatibilité avec les articles 10, 11 et 22 de la Constitution, lus en combinaison avec les articles 6 et 8 de la Convention européenne des droits de l'homme, de l'article 88*quater*, §§ 1er et 3, du Code d'instruction criminelle en ce qu'il sanctionne pénalement l'inculpé qui ne respecte pas l'obligation de fournir des informations visée à l'article 88*quater*, § 1er, du Code d'instruction criminelle, alors que le même inculpé ne peut être sanctionné pénalement s'il ne fournit pas, alors qu'il en est requis, la collaboration à la recherche dans un système informatique au sens de l'article 88*quater*, § 2, du Code d'instruction criminelle.

a été commenté dans le cadre de la précédente chronique. Voy. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, p. 212, n° 297.

1102 Cass. (2e ch.), 4 février 2020, R.G. n° P.19.1086.N, www.cass.be ; *Computerr.*, 2020, p. 278, note D. Van Toor, W. Albers, C. Taylor PArkins-Ozephius et T. Beekhuis, « De ontgrendelplicht in rechtsvergelijkend perspectief » ; *J.T.*, 2020, p. 202, note F. Koning, « Droit au silence et à ne pas s'incriminer : *Quo vadis* ? », *N. C.*, 2020, p. 465 et concl. B. De Smet ; *Rev. dr. pén.*, 2020, p. 1058, note C. Forget, « La compatibilité entre le droit au silence et le fait de contraindre un suspect à dévoiler un "mot de passe" » ; *T. Strafr.*, 2020, p. 219, note C. Conings et R. De Keersmaecker, « To save but not too safe : hoogste Belgische rechters zien geen graten in het decryptiebevel voor de verdachte ».

1103 Cass. (2e ch.), 4 février 2020, R.G. n° P.19.1086.N, point 3.

1104 *Ibid.*, points 4-7.

1105 C.C., arrêt 28/2020, 20 février 2020.

La Cour souligne avant toute chose que l'article 88*quater* du Code d'instruction criminelle prévoit deux types d'obligations[1106] : une obligation d'information à l'égard du juge d'instruction (§ 1er) et une obligation de coopération à la mise en marche du système informatique (§ 2).

Alors que la première obligation s'applique à quiconque ayant une connaissance particulière du système informatique, en ce compris l'inculpé, la seconde obligation s'applique à toute « personne appropriée » à l'exception de l'inculpé. L'exemption prévue par l'article 88*quater*, § 2, alinéa 2, du Code d'instruction criminelle est justifiée au regard du droit de l'inculpé de ne pas s'auto-incriminer et de son droit au silence[1107]. Comme la Cour de cassation l'a souligné dans l'arrêt commenté plus haut, l'obligation d'information établie par l'article 88*quater*, § 1er, du Code d'instruction criminelle à charge de l'inculpé est en revanche parfaitement compatible avec l'article 6 de la Convention. Il découle de la jurisprudence de la Cour européenne des droits de l'homme que les informations recueillies existent dans ce cas indépendamment de la volonté de ce dernier[1108]. La différence de traitement entre les deux obligations – information et coopération – repose donc sur un critère objectif, à savoir la nature de la collaboration qui peut être exigée par le juge d'instruction : dans le premier cas, fournir des informations ; dans le second cas, mettre en fonctionnement un système informatique[1109]. Partant, la différence de traitement est raisonnablement justifiée au regard de l'article 6 de la Convention. À la lumière de ces considérations, la Cour conclut que la question préjudicielle appelle une réponse négative.

D. Mise en place de dispositifs de surveillance dans l'environnement numérique

1. Programmes de surveillance secrète et interception en masse de communications

336. Programme suédois de surveillance électronique de masse. Dans un arrêt rendu le 19 juin 2018 à l'occasion de l'affaire « *Centrum för Rättvisa* »[1110], la Cour européenne des droits de l'homme (troisième section) s'est penchée sur le programme de surveillance électronique de masse mis en place par le gouvernement suédois. La requérante, une organisation suédoise non gouvernementale, craignait que ses communications téléphoniques et Internet sur les réseaux mobiles aient été ou soient un jour interceptées et examinées dans le cadre des activités de renseignement d'origine électromagnétique (ROEM) qui peuvent être menées par l'Institut national (suédois) de la défense radio (« le FRA »).

La Cour européenne des droits de l'homme conclut toutefois à l'unanimité à la non-violation de l'article 8 de la Convention européenne des droits de l'homme après avoir fait application des principes dégagés dans son arrêt rendu en Grande Chambre dans l'affaire *Roman Zakharov*

1106 C.C., arrêt n° 28/2020, 20 février 2020, B.2.3.

1107 Dans un arrêt du 23 juin 2015 commenté dans la précédente chronique « 2015-2017 » (C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, p. 214, n° 300), la cour d'appel de Gand avait déjà rappelé que le « droit au silence » empêche de contraindre un suspect de collaborer activement avec les autorités poursuivantes.

1108 Cour eur. D.H. (gde ch.), arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, req. n° 19187/91, § 69.

1109 C.C., arrêt n° 28/2020, 20 février 2020, B.6.1.

1110 Cour eur. D.H. (3e sect.), arrêt *Centrum för Rättvisa c. Suède*, 19 juin 2018, req. n° 35252/08. Pour un commentaire, voy. not. P. Vogiatzoglou, « "Bulk interception of communications in Sweden meets Convention standards": the latest addition to mass surveillance case law by the European Court of Human Rights », 9 July 2018, https://strasbourgobservers.com (consulté le 22 juin 2021).

c. Russie[1111]. La Cour observe tout d'abord que les mesures d'interception reposent sur une base en droit interne, la législation suédoise sur le renseignement d'origine électromagnétique[1112]. L'existence de règles claires et détaillées en matière d'interception de communications téléphoniques est particulièrement importante puisque « le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret »[1113]. Ensuite, les mesures de surveillance poursuivent des buts légitimes répondant à l'intérêt de la sécurité nationale. Les États membres disposent d'une ample marge d'appréciation afin de choisir le *type de système* d'interception permettant de sauvegarder au mieux la sécurité nationale[1114]. Leur marge de manœuvre est cependant plus restreinte s'agissant de la *mise en œuvre* du système d'interception sélectionné. Celui-ci doit obéir à des « garanties adéquates et effectives contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre »[1115]. En l'occurrence, la Cour européenne des droits de l'homme considère que la législation suédoise offre des garanties suffisantes au regard des critères identifiés : « l'accessibilité du droit interne, le champ d'application du ROEM, la durée des activités de ROEM, l'autorisation des mesures, les procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées, la supervision de l'application de mesures, les mécanismes de notification et les recours prévus par le droit national »[1116].

337. Programme britannique de surveillance électronique de masse. La Cour européenne des droits de l'homme est amenée à se pencher sur la conventionnalité d'un autre programme de surveillance à l'occasion de l'affaire « *Big Brother Watch et autres* ». Des citoyens et des organisations de la société civile, parmi lesquels des associations de journalistes et des journalistes, se plaignent du programme de surveillance électronique mis en œuvre par le gouvernement britannique[1117]. En particulier, ils s'inquiètent de la conformité avec les articles 8 et 10 de la Convention de trois systèmes : le système d'interception massive des communications fondé sur l'article 8(4) de la loi portant réglementation des pouvoirs d'enquête (« la LRPE ») ; le système de partage de renseignements ; le système d'acquisition des données de communication auprès de fournisseurs de services de communication basé sur le chapitre II de la LRPE. Dans un arrêt rendu le 13 septembre 2018, la Cour européenne des droits de l'homme (première section), a jugé que les systèmes d'interception des communications et d'acquisition des données de communication présentent certaines défaillances au regard des garanties attendues à la lumière de l'arrêt précité *Roman Zakharov c. Russie*[1118]. Partant, les deux systèmes violent l'article 8 de la Convention européenne

1111 Cour eur. D.H. (gde ch.), arrêt *Roman Zakharov c. Russie*, 4 décembre 2015, req. n° 47143/06, §§ 228-236. Sur les enseignements de cet arrêt, voy. not. C. Forget et F. Dumortier, « Criminalité informatique – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, pp. 216-2017, n° 305.

1112 Cour eur. D.H. (3e sect.), arrêt *Centrum för Rättvisa c. Suède*, 19 juin 2018, req. n° 35252/08, § 111.

1113 *Ibid.*, § 101.

1114 Cour eur. D.H. (3e sect.), décision *Weber et Saravia c. Allemagne*, 29 juin 2016, req. n° 54934/00, § 106.

1115 *Ibid.*, § 104.

1116 *Ibid.*, § 114.

1117 Cour eur. D.H. (1re sect.), arrêt *Big Brother Watch et autres c. Royaume-Uni*, 13 septembre 2018, req. nos 58170/13, 62322/14 et 24960/15. Pour un commentaire, voy. not. B. van der Sloot et E. Kosta, « Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance – Big Brother Watch and Others v the United Kingdom, Application numbers 58170/13, 62322/14 and 24960/15, Judgment of the European Court of Human Rights of 13 September 2018 », *E.D.P.L.*, 2019/2, pp. 252-261.

1118 Cour eur. D.H. (3e sect.), arrêt *Centrum för Rättvisa c. Suède*, 19 juin 2018, req. n° 35252/08, § 307.

des droits de l'homme. En ce qu'ils peuvent porter sur des éléments journalistiques confidentiels inclus, ces deux systèmes violent également l'article 10 de la Convention. Le système de partage de renseignements n'emporte pas, en revanche, de violation de l'article 8 de la Convention.

338. Affaires portées devant la Grande Chambre de la Cour européenne des droits de l'homme. Les deux affaires ont donné lieu à un arrêt de la Cour européenne des droits de l'homme en Grande Chambre le 25 mai 2021[1119]. Si l'examen de ces deux arrêts déborde de la période étudiée dans le cadre de la présente chronique, quelques mots s'imposent néanmoins.

Dans la première affaire, la Grande Chambre conclut, par quinze voix contre deux, à la violation de l'article 8 de la Convention européenne des droits de l'homme. Affinant les critères à prendre en compte dans l'appréciation de la conformité à la Convention d'un régime national d'interception[1120], elle met l'accent sur la nécessité de prévoir des « garanties de bout en bout » suffisantes pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus[1121]. En l'occurrence, la Cour juge que le processus suédois d'interception n'offre pas de telles garanties. L'absence d'un contrôle *a posteriori* effectif[1122] et la possibilité de partage de renseignements avec des partenaires étrangers sans prendre en compte préalablement les intérêts liés à la vie privée[1123] ont été déterminants. Dans la seconde affaire, la Grande Chambre confirme, à l'unanimité, que la législation britannique n'offre pas de « garanties de bout en bout » suffisantes au regard de l'article 8 de la Convention. Les lacunes constatées sous l'angle de l'article 8 de la Convention participent aux défaillances constatées sous l'angle de l'article 10 de la Convention et, partant, à la violation de ladite disposition[1124].

2. Installation et utilisation de caméras de surveillance par les services de police

339. Régime particulier pour l'enregistrement et le traitement d'images de caméras par les services de police. Par un arrêt du 20 février 2020[1125], la Cour constitutionnelle se penche sur la constitutionnalité de la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière[1126].

1119 Cour eur. D.H. (gde ch.), arrêt *Centrum för Rättvisa c. Suède*, 25 mai 2021, req. n° 35252/08 ; Cour eur. D.H. (gde ch.), arrêt *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, req. n^{os} 58170/13, 62322/14 et 24960/15.

1120 Cour eur. D.H. (gde ch.), arrêt *Centrum för Rättvisa c. Suède*, 25 mai 2021, req. n° 35252/08, § 275.

1121 *Ibid.*, § 264.

1122 *Ibid.*, § 364.

1123 *Ibid.*, §§ 326-328.

1124 En revanche, la Grande Chambre confirme, par douze voix contre cinq, que la réception d'éléments dont l'interception avait été sollicitée auprès de l'Office national de sécurité américain (« la NSA ») n'emporte aucune violation des articles 8 et 10 de la Convention.

1125 C.C., arrêt n° 27/2020, 20 février 2020. Pour un commentaire, voy. not. R. Saelens, « De verzameling en opslag van gegevens door middel van automatic number plate recognition : wat is het probleem? », *T.P.P.*, 2020, liv. 3, pp. 31-37 ; F. Schuermans et L. Keunen, « Grondwettelijk Hof geeft zegen aan politioneel (ANPR) cameragebruik », *Computerr.* (Pays-Bas), 2020, liv. 4, pp. 276-278.

1126 *M.B*, 16 avril 2018.

340. Délai de conservation et droit à la vie privée. La partie requérante estime, tout d'abord, que la possibilité prévue par la loi attaquée de conserver durant douze mois les informations et données à caractère personnel recueillies par les caméras de police en vertu de la loi du 5 août 1992 et de conserver durant trois mois les images enregistrées par des caméras de surveillance constitue une ingérence disproportionnée dans le droit au respect de la vie privée, lequel englobe la protection des données à caractère personnel et des informations personnelles.

Le délai de conservation de douze mois étant un délai maximum, il n'est pas obligatoire de conserver les données durant un tel délai[1127]. Partant, le principe de proportionnalité est respecté[1128]. Le législateur distingue par ailleurs suivant que les données ont été collectées par la police au moyen d'une caméra visible ou non visible[1129].

La Cour rappelle, en outre, la distinction réalisée entre le délai de conservation et le délai d'accès[1130]. Les règles d'accès diffèrent suivant que l'accès a lieu dans le cadre de missions de police administrative ou de missions de police judiciaire[1131]. Dans les deux cas, la demande d'accès doit être dûment motivée[1132].

341. Autorisations, habilitations et droit à la vie privée. La partie requérante s'attaque en outre à quatre mesures en particulier : (i) l'autorisation d'utiliser des caméras de police non visibles, (ii) l'accès des services de police et des services de renseignement et de sécurité aux données conservées sur la base de la loi attaquée, (iii) l'autorisation donnée aux services de police et aux services de renseignement et de sécurité de mettre ces données en corrélation avec d'autres données décrites dans la loi et (iv) l'autorisation donnée aux services de renseignement et de sécurité de procéder, via cet accès et cette corrélation, à une observation en utilisant des moyens techniques.

Force est de constater que les autorisations et habilitations visées sont clairement délimitées dans les dispositions de la loi attaquée. Elles tendent à contribuer à garantir la sécurité publique, à protéger l'ordre public, à prévenir les infractions et à protéger les droits et libertés d'autrui.

1127 *Doc.*, Ch., 2017-2018, n° 54-2855/003, pp. 74-75.

1128 C.C., arrêt n° 27/2020, 20 février 2020, B.9.2.

1129 La Cour constitutionnelle a déjà eu l'occasion de se prononcer sur les données des caméras de reconnaissance automatique des plaques d'immatriculation conservées dans la Banque de données nationale générale et dans les banques de données de base (C.C., arrêt n° 108/2016, 14 juillet 2016, B.112-B.116). Pour un commentaire, voy. not. C. Fievet, L. Gérard, N. Gillart, e.a., « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information – Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3, p. 110, n° 128. Voy. aussi A. Bouvy, M. Borres, M. Solbreux, C. Nennen, P. Nihoul et J. Debry, « La Cour constitutionnelle – Chronique de jurisprudence 2016 », *R.B.D.C.*, 2017/3, p. 251.

1130 C.C., arrêt n° 27/2020, 20 février 2020, B.9.6.

1131 Les missions de police administrative portent en substance sur le maintien de l'ordre public. Les missions de police judiciaire portent en substance sur la recherche et la constatation d'infractions (B.9.6).

1132 L'accès à des fins de police administrative n'est possible que durant un mois à partir de l'enregistrement des données. Passé ce délai, l'accès n'est autorisé qu'à des fins de police judiciaire et moyennant une décision écrite et motivée du procureur du Roi ou, pour ce qui concerne l'utilisation non visible de caméras, du juge d'instruction (articles 25/7 et 46/13 de la loi du 5 août 1992, insérés respectivement par les articles 12 et 61 de la loi du 21 mars 2018). Une distinction encore plus détaillée est réalisée s'agissant de l'accès aux données des caméras de reconnaissance automatique des plaques d'immatriculation. La Cour souligne enfin que le législateur a prévu des mécanismes de contrôle afin de sécuriser les données et informations collectées (C.C., arrêt n° 27/2020, 20 février 2020, B.9.8).

Les mesures répondent donc à un besoin social impérieux dans une société démocratique[1133]. La Cour souligne, par exemple, que l'utilisation de caméras de police non visibles ne peut avoir lieu qu'en raison de circonstances particulières strictement définies par l'article 46/4 de la loi du 5 août 1992, tel qu'inséré par l'article 48 de la loi attaquée. Elle a, du reste, constaté, par son arrêt n° 108/2016 du 14 juillet 2016, que les catégories d'informations de police administrative définies dans l'article 44/5, § 1er, alinéa 1er, 2° et 3°, de la loi du 5 août 1992 sont suffisamment précises[1134]. Les autorisations et habilitations attaquées sont en outre soumises à plusieurs restrictions[1135].

342. Délégation au Roi et principe de légalité. La partie requérante invoque encore la violation du principe de légalité, contenu dans l'article 22 de la Constitution, par l'habilitation étendue conférée au Roi pour régler l'accès direct des services de renseignement et de sécurité aux données recueillies par les services de police à l'aide de caméras[1136]. Après avoir rappelé qu'une délégation à un autre pouvoir n'est pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur, la Cour note que les conditions d'accès ont été réglées de manière précise par le législateur lui-même. Il s'ensuit que l'habilitation est suffisamment précise[1137].

343. Mise en corrélation de données et garanties tirées du droit à un procès équitable. Enfin, la partie requérante estime que la mise en corrélation de données, autorisée par l'article 44/11/3*decies*, § 4, de la loi du 5 août 1992 devrait être soumise aux mêmes garanties que celles prévues par l'article 47*sexies* du Code d'instruction criminelle. Étant donné que la loi du 21 mars 2018 ne prévoit pas davantage un contrôle juridictionnel effectif de la corrélation de données et de l'accès à celles-ci, elle violerait également le droit à un procès équitable et le droit de défense.

L'article 47*sexies*, § 1er, du Code d'instruction criminelle organise l'observation en tant que méthode particulière de recherche (MPR). Or, la mise en corrélation de certaines données n'est pas une méthode particulière de recherche. Alors que l'observation tend, en général, à recueillir de nouvelles données, la mise en corrélation porte sur des données existantes, qui sont recueillies d'une manière qui est, en l'espèce, entourée de garanties suffisantes (notamment les principes de finalité et de proportionnalité, supportés par le principe de distinction). Il est dès lors raisonnablement justifié que les deux techniques ne soient pas soumises aux mêmes garanties[1138]. En outre, la Cour souligne que toutes les informations et données à caractère personnel qui sont traitées par les services de police peuvent être contrôlées par une autorité de contrôle indépendante de l'information policière, créée auprès de la Chambre des représentants, dénommée Organe de

1133 *Ibid.*, B.14.1.

1134 *Ibid.*, B.20-B.32.

1135 *Ibid.*, B.14.2-B.14.6. La partie requérante contestait aussi l'habilitation étendue conférée aux ministres de l'Intérieur et de la Justice pour prendre des mesures en ce qui concerne l'interconnexion et la corrélation avec les banques de données techniques. Celle-ci n'a cependant pas été examinée dans la mesure où la disposition sur laquelle elle repose – l'article 44/4, § 4, de la loi du 5 août 1992, inséré par l'article 28 de la loi du 21 mars 2018 – a été remplacée, sans avoir eu l'occasion d'être appliquée, par l'article 7 de la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière ».

1136 Article 84 de la loi du 21 mars 2018.

1137 *Ibid.*, B.17-B.19.3.

1138 *Ibid.*, B.21.3.

contrôle de l'information policière[1139] (article 44/1 de la loi du 5 août 1992). Toutes les banques de données policières relèvent, en outre, du pouvoir de contrôle de cet organe qui exerce un pouvoir de contrôle général (article 44/2 de la loi du 5 août 1992). La Cour a déjà eu l'occasion de formuler ces observations dans son arrêt n° 153/2018 du 8 novembre 2018[1140].

Au demeurant, si la mise en corrélation ne relève pas du contrôle de la chambre des mises en accusation lors de la clôture d'une instruction puisqu'elle ne constitue pas une méthode particulière de recherche, elle peut être soumise, comme toute décision prise par une autorité publique, au contrôle du juge[1141].

3. Installation et utilisation de caméras de surveillance par d'autres personnes que des fonctionnaires de police

344. Utilisation d'images de vidéosurveillance sur le lieu de travail à d'autres fins que celles pour lesquelles elles ont été obtenues. Dans un arrêt du 28 novembre 2018, la cour d'appel de Bruxelles se prononce sur une utilisation d'images de vidéosurveillance sur le lieu de travail constatant fortuitement des infractions pénales[1142].

Le prévenu considérait que la plainte avec constitution de partie civile déposée à son encontre se fondait sur une utilisation illégale des images de vidéosurveillance obtenues par Mont-de-Piété de la société de sécurité privée à laquelle il fait appel (Securitas). Une telle utilisation ne serait pas prévue par les ordres de service du Mont-de-Piété, serait contraire à la convention collective de travail n° 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail et violerait le droit à la vie privée du prévenu, tel que garanti par l'article 8 de la Convention.

La cour d'appel de Bruxelles constate, à la suite du premier juge, que les dispositions citées n'ont nullement été violées. En particulier, elle remarque que les principes de finalité, de proportionnalité et de transparence ont été respectés dès l'instant où les employés étaient informés de l'existence de caméras qui étaient, de surcroît, parfaitement visibles. La circonstance que le dispositif de vidéo-surveillance ait été placé, non pas pour assurer la surveillance du personnel et le contrôle des prestations, mais pour garantir la protection des travailleurs, des biens et du bâtiment, n'empêche aucunement « de faire usage des images dans le cadre d'une plainte auprès des autorités judiciaires lorsqu'une infraction est constatée de manière fortuite, comme en l'espèce, lors du visionnage des images »[1143]. Quoi qu'il en soit, la Cour rappelle l'applicabilité de la jurisprudence « Antigone » en droit pénal social. Même si la preuve était illégale – *quod non* – elle ne pourrait être écartée par le juge que dans trois hypothèses qui ne se présentent pas en l'espèce : soit que la règle de droit dont la violation est avancée était prescrite à peine de nullité, soit que le vice invoqué a entaché la fiabilité de la preuve querellée, soit que l'illégalité invoquée a compromis le droit du prévenu à un procès équitable.

1139 Organe visé à l'article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel.

1140 Voy. C.C., 8 novembre 2018, n° 153/2018, commenté *supra*, n^os^ 326-328.

1141 *Ibid.*, B.21.5.

1142 Bruxelles (11^e^ ch.), 28 novembre 2018, 2014/CO/201, *Dr. pén. entr.*, 2019/4, pp. 299-302.

1143 Bruxelles (11^e^ ch.), 28 novembre 2018, 2014/CO/201, *Dr. pén. entr.*, 2019/4, p. 300, point 5.

345. Installation et utilisation de caméras de surveillance dans des lieux qui présentent un risque particulier pour la sécurité. Dans l'arrêt précité du 20 février 2020[1144], la Cour constitutionnelle se penche également sur les modifications apportées par la loi du 21 mars 2018 à la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance. La loi du 21 mars 2018 prolonge le délai de conservation des données jusqu'à trois mois pour les lieux qui, par leur nature, présentent un risque particulier pour la sécurité. La Cour constitutionnelle est, ici aussi, sensible au principe de distinction, soulignant que la loi du 21 mars 2007, telle que modifiée par la loi attaquée, établit une distinction entre les caméras de surveillance fixes – permanentes ou temporaires – et les caméras de surveillance mobiles, et prévoit un régime distinct selon la nature du lieu où la caméra est utilisée (lieu ouvert, lieu fermé accessible au public, lieu fermé non accessible au public)[1145]. Elle souligne également les restrictions qui encadrent les différents régimes. L'enregistrement de données continue d'être balisé par le principe de finalité, n'étant autorisé que « dans le but précis de recueillir des preuves d'incivilités ou de faits qui sont constitutifs d'infractions ou générateurs de dommages et de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes »[1146]. Il respecte aussi le principe de proportionnalité en ce qu'il constitue un délai exceptionnel et maximal. Le délai de conservation ordinaire reste toujours, par ailleurs, d'un mois au maximum. Au demeurant, il appartient, au Roi, par un arrêté royal délibéré en Conseil des ministres et après Avis de l'Autorité de protection des données, de déterminer les lieux « qui, par leur nature, présentent un risque particulier pour la sécurité ». Il ressort des travaux parlementaires que l'on vise les gares, les aéroports et les infrastructures portuaires, « ou d'autres lieux susceptibles de constituer une cible pour les terroristes, comme les lieux où les agents de gardiennage peuvent exercer leurs compétences situationnelles, tels que les sites nucléaires, les institutions internationales, les domaines militaires, etc. »[1147].

E. Fait justificatif « du lanceur d'alerte »

346. Affaire « *Lux Leaks* ». Dans un arrêt du 15 mai 2018, la Cour d'appel du Grand-Duché du Luxembourg se prononce sur l'affaire « *Lux Leaks* »[1148] Un arrêt de la Cour européenne des droits de l'homme (troisième section) a récemment été rendu dans cette même affaire[1149].

1144 C.C., arrêt n° 27/2020, 20 février 2020. Pour un commentaire, voy. not. R. Saelens, « De verzameling en opslag van gegevens door middel van automatic number plate recognition : wat is het probleem? », *T.P.P.*, 2020, liv. 3, pp. 31-37 ; F. Schuermans et L. Keunen, « Grondwettelijk Hof geeft zegen aan politioneel (ANPR) cameragebruik », *Computerr.* (Pays-Bas), 2020, liv. 4, pp. 276-278.

1145 *Ibid.*, B.10.1.

1146 C.C., arrêt n° 27/2020, 20 février 2020, B.10.6.

1147 *Doc.*, Ch., 2017-2018, n° 54-2855/001, pp. 18 et 77 et n° 54-2855/003, p. 11.

1148 Pour un commentaire du traitement de cette affaire par les juges luxembourgeois, voy. not. E. Cobbaut, « L'encadrement de l'alerte et la protection du lanceur d'alerte (whistleblower) : l'affaire *Luxleaks* à l'aune d'un cadre européen en construction », *R.D.T.I.*, 2019/2, pp. 47-85 ; M. Nelles, « Le procès Luxleaks, prémices d'un retournement de situation en faveur des lanceurs d'alerte ? », *J.L.M.B.*, n° 38, 2018, pp. 1803-1806 ; A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale : de la complaisance à la vigilance*, Bruxelles, Larcier, 2021, n^os^ 680 et s.

1149 Cour eur. D.H. (3^e^ sect.), arrêt *Halet c. Luxembourg*, 11 mai 2021, req. n° 21884/18. Pour un premier commentaire, voy. not. justice-en-ligne V. Junod, « "Lanceurs d'alerte : oui, mais à vos risques et périls !". Telle est la leçon de la jurisprudence actuelle de la Cour européenne des droits de l'homme », 2 juin 2021, https://www.justice-en-ligne.be (consulté le 23 juin 2021).

L'affaire « *Lux Leaks* » débute avec la diffusion d'un reportage du magazine *Cash Investigation* sur la chaîne de télévision *France 2*[1150]. Le reportage met en scène une demande de rescrit fiscal avec l'entête de *PricewaterhouseCoopers* accompagnée d'une lettre d'accord de l'administration fiscale luxembourgeoise. Les documents proviennent d'un ancien salarié de PwC, Antoine Deltour[1151]. Le reportage est suivi d'un second reportage, quelques mois plus tard, qui contient de nouvelles révélations sur la base de déclarations fiscales de clients de PwC[1152]. Celles-ci proviennent d'un autre salarié du cabinet d'audit, Raphaël Hallet. Les informations se retrouvent ensuite publiées dans la presse et sur le site Internet du Consortium International de Journalistes d'Investigation. Dans les deux cas, les données dérobées ont été confiées à un journaliste français, Edouard Perrin. Le 5 juin 2012, la société PwC porte plainte auprès du Parquet de Luxembourg du chef de vol, violation du secret professionnel et blanchiment-détention.

En première instance[1153], la section correctionnelle du Tribunal d'arrondissement de Luxembourg estime qu'« il n'existe aucune protection au niveau européen ». Le juge luxembourgeois condamne alors les deux travailleurs du chef des infractions retenues à leur charge[1154]. Le journaliste est en revanche relaxé. La Cour d'appel du Grand-Duché de Luxembourg ne partage pas l'avis du Tribunal d'arrondissement de Luxembourg, accueillant en faveur d'Antoine Deltour, au regard de la jurisprudence de la Cour européenne des droits de l'homme[1155], la cause justificative du « lanceur d'alerte ». Après avoir admis que l'article 10 de la Convention européenne des droits de l'homme s'applique au cas d'espèce, le juge luxembourgeois considère que la liberté d'expression « consacrée par un texte supranational, ne saurait être mise en échec par les règles nationales internes. Ainsi, dans le cadre d'un débat sur une question d'intérêt général portant sur l'évitement fiscal, la défiscalisation et l'évasion fiscale, la liberté d'expression du lanceur d'alerte peut, le cas échéant et sous certaines conditions, prévaloir et être invoquée comme fait justifiant la violation de la loi nationale ». En l'occurrence, la Cour luxembourgeoise accueille le fait justificatif du lanceur d'alerte quant à l'infraction de violation du secret professionnel établie dans le chef d'Antoine Deltour. Les autres préventions – à savoir le vol domestique et la fraude informatique – sont, en revanche, établies au motif que le prévenu n'a pas agi, au moment de la commission de ces infractions, avec l'« *animus* » du lanceur d'alerte. En revanche, la Cour d'appel luxembourgeoise

1150 Sur les faits à l'origine de l'affaire « *Lux Leaks* », voy. A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale, op. cit.*, n^os^ 180 et s.

1151 Antoine Deltour a dérobé plus de 45.000 pages de documents de formations internes et des documents concernant des « *Advanced Tax Agreements* » (des ATAs) de 400 clients de la société *PricewaterhouseCoopers*, approuvés par l'Administration des contributions directes du Luxembourg.

1152 Raphaël Hallet a soustrait 16 déclarations fiscales (« *Tax returns* ») de clients de la société *PricewaterhouseCoopers*.

1153 Tribunal d'arrondissement de Luxembourg (12^e^ ch.), jugement du 29 juin 2016, disponible sur www.justice.public.lu (consulté le 25 juin 2021).

1154 Antoine Deltour est condamné du chef des infractions retenues à sa charge à une peine d'emprisonnement de 12 mois, à une amende de 1.500 euros ainsi qu'aux frais de sa poursuite pénale. Raphaël Halet est condamné du chef des infractions retenues à sa charge à une peine d'emprisonnement de 9 mois, à une amende de 1.000 euros ainsi qu'aux frais de sa poursuite pénale.

1155 Cour eur. D.H. (gde ch.), arrêt *Guja c. Moldova*, 12 février 2008. Pour un commentaire de l'arrêt *Guja*, voy. V. Junod, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande Chambre), *Guja c. Moldova*, 12 février 2008 », *Rev. trim. dr. h.*, n° 77, 2009, pp. 227-260. Voy. aussi D. Voorhoof et T. Gombeer, « Dénoncer des irrégularités à la police et la justice est l'exercice de la liberté d'expression », *Vigiles*, 2008, liv. 5, pp. 253-259 ; M. Daelemans, « E.H.R.M. 12 februari 20083 », *R.W.*, 2010-2011, n° 6, pp. 251-253 ; D. Voorhoof, « Europees Hof neemt klokkenluider in bescherming », *De Juristenkrant*, n° 167, 2008, pp. 1 et 3.

refuse de reconnaitre à Raphaël Hallet le statut protecteur du lanceur d'alerte au motif que les documents transmis au journaliste français ne font qu'illustrer, sans rien apporter de nouveau, un débat public déjà initié par les révélations d'Antoine Deltour, quelques mois auparavant.

L'exigence d'un élément moral afin de pouvoir bénéficier du fait justificatif du lanceur d'alerte a retenu l'attention de la Cour de cassation du Grand-Duché de Luxembourg dans le cadre du pourvoi formé par Antoine Deltour contre la décision du juge d'appel[1156]. Le pourvoi formé par Raphaël Hallet a, de son côté, été rejeté. Considérant que « la reconnaissance du statut de lanceur d'alerte doit s'appliquer en principe à toutes les infractions du chef desquelles une personne, se prévalant de l'exercice de son droit garanti par l'article 10 de la Convention, est poursuivie, sous peine de vider la protection devant résulter du statut de lanceur d'alerte de sa substance », la haute juridiction a invalidé l'élément moral requis par le juge luxembourgeois.

La Cour d'appel luxembourgeoise, selon une nouvelle composition, a réexaminé la condamnation d'Antoine Deltour à la lumière des éléments de droit tranchés par la Cour de cassation. Dans son arrêt du 15 mai 2018, elle neutralise l'ensemble des « faits en rapport avec l'appréhension antérieure des documents de rescrits fiscaux en octobre 2010 à Luxembourg, qualifiée respectivement de vol domestique, de maintien frauduleux dans un système informatique et de blanchiment-détention de l'objet du vol domestique », conformément à l'arrêt de la Cour de cassation[1157]. En revanche, les infractions en rapport avec l'appréhension des documents de formation interne sont établies[1158].

[1156] Cour de cassation du Grand-Duché de Luxembourg, arrêt du 11 janvier 2018 dans le cadre de l'affaire dite « *LuxLeaks* », disponible sur https://justice.public.lu (consulté le 25 juin 2021). Pour un commentaire, voy. M. Nelles, « Le procès Luxleaks, prémices d'un retournement de situation en faveur des lanceurs d'alerte ? », *J.L.M.B.*, n° 38, 2018, pp. 1803-1806 ; Th. Postif, « L'affaire *Luxleaks*. L'extension de la protection des lanceurs d'alerte à toutes les infractions qui leur sont reprochées », *Semaine Juridique Entreprise et affaires*, supplément, 2018, n° 13.

[1157] Cour d'appel du Grand-Duché du Luxembourg (5e ch.), arrêt du 15 mai 2018, affaire dite « *LuxLeaks* », disponible sur le site www.justice.public.lu (consulté le 25 juin 2021).

[1158] La Cour d'appel ordonne cependant la suspension du prononcé pour trois ans mais confirme la décision du tribunal d'arrondissement condamnant Antoine Deltour à payer un euro symbolique à son employeur.