V. CRIMINALITÉ INFORMATIQUE

Franck Dumortier[1264] et Catherine Forget[1265]

A. Droit matériel

1. Faux en informatique

269. Faux en informatique et commentaires anonymes sur internet. Le faux en informatique requiert une altération de la vérité par l'introduction, la modification ou l'effacement de données stockées, traitées ou transmises par un système informatique ou par la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique[1266]. Comme pour le faux en écritures de droit commun, il est requis que les données manipulées aient une portée juridique[1267]. En l'espèce, un individu avait posté un ensemble de messages injurieux sur le site internet www.zoekadvocaat.be en se présentant faussement comme un client de deux avocats[1268]. Ces derniers s'étaient, sur cette base, constitués partie civile entre les mains du juge d'instruction pour faux informatique et harcèlement («*stalking*»). Pour examiner la portée juridique des données manipulées, la Cour examine si les faits ont été commis de manière à tromper le lecteur en adoptant une apparence crédible et raisonnable et en ce sens, peut s'imposer à la confiance publique. En l'occurrence, la Cour estime que l'internaute est en principe suffisamment familiarisé avec la valeur relative des messages postés sur ce type de forum et les lit avec prudence, en particulier compte tenu de leur nature subjective et de leur caractère anonyme. Selon la Cour, il est peu probable que ces messages aient pu convaincre de leur véracité et ou de leur exactitude de sorte qu'ils n'avaient une portée juridique que très limitée. Il ne s'agit donc pas d'un faux en informatique.

270. L'usage du faux en informatique doit être apprécié en fait. L'article 210*bis*, § 2, du Code pénal ne définit pas ce qu'il y a lieu entendre par «usage» de faux en informatique. Dès lors, il appartient au juge d'apprécier en fait ce qui constitue cet usage et notamment de vérifier si celui-ci continue à tromper autrui ou à lui nuire et ainsi à produire l'effet voulu par le faussaire[1269].

271. Faux en informatique et interdiction faite à certains condamnés et aux faillis d'exercer certaines fonctions, professions ou activités. L'article 1er, d), de l'arrêté royal n° 22 du 24 octobre 1934 relatif à l'interdiction judiciaire faite à certains condamnés et aux faillis d'exercer certaines fonctions, professions ou activités dispose que le juge qui condamne une personne, même conditionnellement, comme auteur ou complice de faux et usage de faux en écritures ou de tentative de cette infraction peut assortir sa condamnation de l'interdiction d'exercer, personnellement ou par interposition de personne, les fonctions énoncées à cette disposition. Cette disposition n'est pas prévue pour le faux en informatique. Toutefois selon la Cour de cassation, dès lors que,

1264 Chercheur et maître de conférences au CRIDS.
1265 Avocate au barreau de Bruxelles et chercheuse au CRIDS.
1266 Art. 210*bis* du Code pénal.
1267 À ce sujet, voy. O. Leroux, «Section 1. – Criminalité informatique spécifique», in *Les infractions*, vol. 1, Bruxelles, Larcier, 2016, pp. 448-508.
1268 Gand, 19 mai 2015, *R.A.B.G.*, 2016. Pour un commentaire, voy. V. Vereecke, «Anonieme internetcommentaren dringen zich niet op aan het openbaar vertrouwen», *R.A.B.G.*, 2016/1, pp. 73-76.
1269 Cass., 23 mars 2016, R.G. n° P.16.0074.F, www.cass.be.

d'une part, les éléments constitutifs essentiels du faux visé à l'article 210*bis* du Code pénal correspondent à ceux des faux prévus aux articles 194 à 197 dudit Code et que, d'autre part, il ressort de la genèse légale de l'article 210*bis* du Code pénal que le législateur avait l'intention de punir autant que possible de la même manière la criminalité hors ligne et en ligne et de veiller à ce que les infractions existantes ayant recours à l'informatique comme nouveau *modus operandi* ne restent pas impunies, l'article 1er, d), de l'arrêté royal nº 22 du 24 octobre 1934 constitue le fondement légal pour imposer l'interdiction professionnelle dont il est ici question, non seulement à la personne reconnue coupable d'un faux mais également à la personne reconnue coupable de faux en informatique[1270]. Par ailleurs, la Cour précise que le fait que l'article 1er, d), de l'arrêté royal nº 22 du 24 octobre 1934 n'a pas été adapté à l'occasion de l'insertion de l'article 210*bis* du Code pénal par l'article 4 de la loi du 28 novembre 2000 relative à la criminalité informatique n'y fait pas obstacle.

2. Fraude informatique

272. La fraude informatique et l'abus de confiance. Selon l'article 504*quater*, § 1er, du Code pénal, commet une fraude informatique, celui qui cherche à se procurer, pour lui-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. En l'espèce, une employée avait utilisé à des fins privées une carte essence mise à sa disposition par son employeur à des fins professionnelles. Selon la Cour de cassation, il s'agit d'une fraude informatique au sens de l'article 504*quater*, § 1, du Code pénal, et non d'un abus de confiance[1271].

273. La fraude informatique est étrangère à la cause d'excuse absolutoire de parenté en matière de *vol*. L'article 462, alinéa 1er, du Code pénal prévoit que les vols commis au préjudice d'un ascendant, époux et conjoint et autres proches ne donneront lieu qu'à des réparations civiles. Cette immunité familiale s'applique également aux délits d'abus de confiance, d'escroquerie et de tromperie[1272]. Comme le soulève l'avocat général dans ses conclusions, « il existe une controverse sur le caractère des immunités familiales : d'aucuns classent les immunités familiales parmi les exceptions au caractère pénal d'un comportement incriminé (immunité pénale), d'autres les considèrent comme des excuses absolutoires ». S'il s'agit d'une cause d'excuse, il y a lieu de tenir compte de l'article 78 du Code pénal en vertu duquel nul crime ou délit ne peut être excusé, si ce n'est dans les cas déterminés par la loi ; par conséquent la fraude informatique n'est pas visée. En revanche, s'il s'agit d'une immunité pénale, elle s'applique aux atteintes portées au droit de propriété de manière générale compte tenu de la *ratio legis* de la disposition, à savoir préserver la paix des familles[1273]. La Cour de cassation a toutefois opté pour la première option et a considéré

1270 Cass., 13 décembre 2016, R.G. nº P.15.1117.N, www.cass.be.
1271 Anvers, 30 septembre 2015, *N. C.*, 2016, p. 272.
1272 Art. 492 et 504 du Code pénal.
1273 A. Lorent, « L'immunité familiale en matière d'atteintes à la propriété », *Rev. dr. pén. crim.*, 2000, p. 144.

que cette immunité ne s'applique pas en cas de fraude informatique commise au préjudice d'un ascendant, en l'espèce, la mère du demandeur[1274].

3. *Hacking*

274. Le hacking interne est étranger au détournement de la finalité. L'article 550*bis* du Code pénal distingue deux formes d'accès illégal aux systèmes d'information. Le second paragraphe de cette disposition incrimine le *hacking interne* – soit le fait d'un individu, disposant d'un droit d'accès sur le système visé, de dépasser les limites de son autorisation avec une intention frauduleuse – tandis que le premier paragraphe, dédié au *hacking externe*, rend coupable celui qui, étranger au système visé et sachant qu'il n'y est pas autorisé, accède dans ledit système ou s'y maintient[1275]. En l'espèce, la demanderesse était employée du service informatique d'une ville belge et disposait d'un accès illimité à l'ensemble du système informatique de cette ville à des fins d'assistance technique, de maintenance et de dépannage. La Cour de cassation considère que le fait d'accéder à certaines données à des fins totalement différentes et étrangères à son pouvoir ne constitue pas un hacking interne. En effet, la personne concernée disposait d'un pouvoir d'accès aux systèmes et n'a donc pas outrepassé son pouvoir d'accès[1276], le fait que les données aient été utilisées à d'autres fins que celles autorisées initialement est sans incidence. Un tel agissement doit, par contre, être considéré comme une violation du principe édicté à l'article 29 du règlement général sur la protection des données (ci-après « RGPD ») selon lequel « le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre ».

4. *Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique*

275. Principe général de l'interdiction des écoutes. En principe, il est interdit de prendre connaissance du contenu des communications électroniques sans en avoir l'autorisation. En effet, le secret des communications est une facette du droit à la vie privée protégé par l'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution. De plus, les articles 259*bis* et 314*bis* du Code pénal et l'article 124 de la loi du 13 juin 2005 incriminent le fait, pour un tiers, de prendre connaissance d'une communication, d'enregistrer des communications privées pendant leur transmission à l'aide d'un appareil quelconque. Les articles 259*bis* et 314*bis* du Code pénal précisent que ces informations doivent être « en cours de transmission », c'est-à-dire sur le trajet entre l'émetteur et le récepteur[1277].

1274 Cass., 26 avril 2017, R.G. n° P.16.0924.F, www.cass.be. Cette interprétation a été critiquée par la doctrine, voy. F. Kuty, « L'inapplicabilité de l'immunité pénale de parenté ou l'alliance à la fraude informatique, une occasion manquée », *J.L.M.B.*, 2017/23, pp. 1104-1108.

1275 Pour une étude des éléments constitutifs de ces deux formes de hacking, voy. O. Leroux, « Criminalité informatique », in *Les infractions contre les biens*, Bruxelles, Larcier, 2008, pp. 410 et s.

1276 Cass., 24 janvier 2017, R.G. n° P.16.0048.N, *T. Strafr.*, 2017/3, pp. 206-207.

1277 Exposé des motifs, *Doc. parl.*, Sénat, 1992-1993, n° 843/1, p. 6.

276. Interception d'une communication par une personne y prenant part. Dans un arrêt du 17 novembre 2015[1278], dans la ligne de sa jurisprudence antérieure[1279], la Cour de cassation dit pour droit qu'une personne prenant connaissance et enregistrant le contenu d'une communication à laquelle elle participe, sans l'accord de son interlocuteur, n'agit pas dans une intention frauduleuse ou à dessein de nuire lorsqu'elle cherche à se ménager la charge de la preuve. Il ne s'agit par ailleurs pas d'un détournement des articles 90*ter* et suivant du Code d'instruction criminelle, à savoir l'interception des communications non accessibles au public dont la compétence relève du juge d'instruction.

277. Production d'un courrier électronique à des fins probatoires. Dans un contexte non informatique, le secret des lettres et de la correspondance est protégé par les articles 29 de la Constitution et 460 du Code pénal. Cette garantie n'est toutefois pas applicable une fois le courrier reçu par son destinataire[1280]. En l'occurrence, la cour d'appel avait décidé d'écarter des reproductions sur papier de courriels échangés entre une tierce personne et l'une des parties considérant que ces pièces ne pouvaient être admises à titre probatoire. En effet, les documents avaient été obtenus sans intervention policière, en violation du secret des communications et leur authenticité contestée n'avait pas donné lieu à des vérifications, ces lacunes engendrant une atteinte grave à la fiabilité de ces documents. La Cour de cassation considère toutefois qu'aucune disposition légale ne s'oppose à ce que le contenu d'un courrier électronique régulièrement reçu par son destinataire et communiqué à la justice soit admis au titre de preuve par le juge[1281]. De plus, la Cour rappelle que « l'atteinte à la fiabilité de la preuve n'est une cause d'écartement de celle-ci que si elle est imputable à l'illégalité ou à l'irrégularité de l'acte qui en a permis l'obtention »[1282].

278. Atteinte à la vie privée, critère des attentes raisonnables et secret professionnel. Pour apprécier si l'enregistrement d'une conversation porte atteinte au droit au respect de la vie privée, il appartient au juge du fond, sur la base des éléments des faits de la cause, de tenir compte du critère des atteintes raisonnables, c'est-à-dire de prendre en considération le contenu et les circonstances dans lesquelles la conversation a eu lieu[1283]. À ce propos, les qualités des intervenants et du destinataire de l'enregistrement sont déterminantes[1284]. Le secret professionnel pénalement sanctionné par l'article 458 du Code pénal n'interdit pas à un client d'enregistrer une conversation ayant lieu dans le cabinet de son conseil entre lui-même, son conseil et un tiers et d'utiliser cet enregistrement si cela s'avère nécessaire à sa défense dans une procédure pénale engagée notamment contre ce conseil[1285].

1278 Cass., 17 novembre 2015, R.G. n° P.15.0880.N, et concl. av. gen. A. Winants, *N. C.*, 2017, p. 57 ; *Rev. trim. dr. fam.*, 2016, p. 263.

1279 Cass., 9 septembre 2008, R.G. n° P.08.0276.N, *Pas.*, 2008, n° 458 et Cass., 8 janvier 2014, R.G. n° P.13.1935.F, www.cass.be.

1280 Cass., 21 octobre 2009, R.G. n° P.09.0766.F, *Pas.*, 2009, n° 599.

1281 Cass., 22 avril 2015, R.G. n° P.14.1462.F, www.cass.be.

1282 *Ibid.*

1283 Cass., 17 novembre 2015, R.G. n° P.150880.N/1, www.cass.be.

1284 Cass., 7 juin 2016, R.G. n° P.16.0294.N, *Pas.*, 2016/6-7-8, pp. 1362-1366.

1285 Cass., 17 novembre 2015, R.G. n° P.150880.N/1 ; V. Vereecke, « De gespreksopname van een consultatie bij een advocaat », *R.A.B.G.*, 2016/7, pp. 520-524. Au sujet de cet arrêt, voy. également le n° 172 de la présente chronique.

5. La possession d'images à caractère pédopornographique

279. La possession d'images à caractère pédopornographique ne requiert pas de maîtriser leur téléchargement ou leur impression. L'article 383*bis*, § 2, du Code pénal punit quiconque aura sciemment possédé les emblèmes, objets, films, photos, diapositives ou autres supports visuels à caractère pédopornographique ou y aura, en connaissance de cause, accédé par un système informatique ou par tout moyen technologique. En l'espèce, le demandeur en cassation faisait valoir que les images à caractère pédopornographique avaient été trouvées dans un fichier internet temporaire de son ordinateur. Selon ce dernier, il n'avait pas conscience de détenir de tels fichiers et images soulignant que le téléchargement dans un fichier temporaire ne requiert aucune manipulation de l'utilisateur. La Cour de cassation a néanmoins considéré que l'article 383*bis*, § 2, du Code pénal ne requiert pas que l'utilisateur dispose d'une maîtrise des images par le téléchargement ou l'impression[1286]. Il suffit que la personne concernée consulte sciemment un site web et visionne ces images[1287], ce qui ne pouvait être contesté eu égard au nombre de photographies de nature pédopornographique retrouvées mais aussi compte tenu de l'expérience du demandeur en tant qu'utilisateur d'internet.

6. Voyeurisme

280. Attentat à la pudeur et voyeurisme. À plusieurs reprises, il a été rappelé par les cours et tribunaux que le fait de filmer dans leur intimité, des personnes, sans leur consentement, à leur insu, sans contrainte physique ou morale, ne constitue pas un attentat à la pudeur commis avec violences ou menaces au sens de l'article 373 du Code pénal[1288]. Depuis l'adoption de la loi du 1er février 2016[1289], ce type de comportement est expressément sanctionné en vertu de l'article 371/1, 1°, du Code pénal incriminant le voyeurisme[1290].

B. Procédure pénale dans le domaine informatique

1. La saisie de données informatiques

281. La saisie de données informatiques, une mesure découlant de la recherche dans un système informatique. *Avant* l'adoption de la loi du 25 décembre 2016, la procédure en vigueur prévoyait une distinction entre la saisie de données informatiques, relevant de la compétence du procureur du Roi, et la recherche ou l'extension de recherche dans un système informatique, relevant de la compétence du juge d'instruction[1291]. Ce régime faisait l'objet de controverses, le Code d'instruction criminelle ne précisant pas si les enquêteurs pouvaient exploiter un système

1286 Cass., 3 février 2015, R.G. n° P.13.2017.N/3, www.cass.be.

1287 Cass., 20 avril 2011, R.G. n° P.10.2006.F, *Pas.*, 2011, n° 267.

1288 Cass., 31 mars 2015, R.G. n° P.14.0293, *T. Strafr.*, 2015, p. 142, note T. Decaigny, « De strafrechtelijke aanpak van voyeurisme », *N. C.*, 2015, p. 326 ; *J.L.M.B.*, p. 746, obs. A. De Nauw, « Les limites de l'incrimination classique de l'attentat à la pudeur » ; Anvers, 6 mai 2015, *T. Strafr.*, 2015, p. 147 ; Mons, 6 janvier 2016, n° 2015/H/330.

1289 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.

1290 À ce propos, voy. A. Dierckx, « Noopt nieuwe seksuele criminaliteit tot nieuwe seksuele misdrijven? », *N. C.*, 2017, pp. 207-239 ; B. Spriet et J. Boeckxstaens, « Het nieuwe misdrijf van voyeurisme en een aanpassing van het misdrijf van aanranding van de eerbaarheid en van verkrachting », *T. Strafr.*, 2016/3, pp. 207-223 ; I. Wattier, « La nouvelle incrimination de voyeurisme et l'extension de l'attentat à la pudeur et du viol », *Rev. dr. pén.*, 2018/2, p. 119.

1291 Art. 39*bis* CICr et 88*ter* CICr.

informatique sans disposer d'une ordonnance du juge d'instruction. La question fut tranchée par la Cour de cassation dans un arrêt du 11 février 2015. La Cour dit pour droit que « l'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous la forme d'un sms, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête »[1292]. Cette jurisprudence fut entérinée par la loi du 25 décembre 2016[1293], faisait fi de la nécessité de distinguer la « saisie » de données de la « recherche » dans un système informatique dont la portée de l'ingérence dans le droit au respect de la vie privé diffère[1294].

282. L'interdiction des saisies « massives et indifférenciées » et le droit à un recours effectif. L'affaire *Vinci Construction et GTM génie civil et services c. France* est l'occasion pour la Cour européenne des droits de l'homme de rappeler qu'une saisie ne peut être « massive et indifférenciée ». En l'espèce, une saisie avait été opérée par des enquêteurs de la Direction générale de la concurrence, de la consommation et de la répression des fraudes dans deux entreprises et de nombreuses correspondances entre un avocat et son client avaient été saisies. En examinant les garanties offertes aux intéressées, la Cour relève, d'une part, que les enquêteurs ont essayé de circonscrire leurs fouilles aux documents détenus par les employés travaillant dans le domaine d'activité concerné et, d'autre part, qu'un inventaire suffisamment précis ainsi qu'une copie des fichiers saisis ont été remis aux requérantes lesquels constituent des garanties suffisantes. En effet, selon la Cour, sur cette base, les intéressés étaient en mesure de vérifier que seules les données en lien avec l'objet de l'enquête avaient été emportées de sorte qu'il ne s'agissait pas d'une saisie « massive et indifférenciée » susceptible d'emporter la violation de la Convention[1295]. En revanche, une mesure n'organisant pas de recours effectif pourrait emporter la violation de l'article 8 de la CEDH, les personnes concernées ne pouvant mettre en cause la régularité de la saisie et le juge, en contrôler la légalité et si nécessaire ordonner la restitution voire l'effacement des documents saisis[1296].

2. La recherche et l'extension de recherche dans un système informatique

283. La recherche dans un système informatique et l'autorisation préalable d'un organe indépendant. La Cour européenne des droits de l'homme a rarement été confrontée à des litiges relatifs à une saisie de données indépendamment d'une perquisition dans un lieu réel et opère donc souvent une certaine confusion entre saisie, recherche et perquisition. Dans l'arrêt *Trabajo*

1292 Cass., 11 février 2015, R.G. n° P.14.1739.F, www.cass.be. Pour un commentaire d'arrêt, voy. C. Conings, « Het uitlezen van een gsm of een ander privaat IT-systeem: This is not America », note sous Cass., 11 février 2015, *R.W.*, 2015-2016, pp. 622-626.

1293 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.

1294 Pour un commentaire, voy. C. Conings et S. Royer, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *N. C.*, 2017/4, pp. 313-320 ; V. Franssen et S. Tosza, « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », in *Les droits des justiciables face à la justice pénale*, Limal, Anthemis, 2017, p. 226 ; C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ? », *R.D.T.I.*, à paraître, 2018.

1295 Cour eur. D.H., 2 avril 2015, *Vinci construction et GMT Génie Civil et services c. France*, n^{os} 63629/10 et 60567/10.

1296 Cour eur. D.H., 21 mars 2017, *Société Janssen Cilag c. France*, n° 33931/12, § 23.

Rueda[1297], la Cour semble implicitement reconnaître qu'une recherche dans un système informatique requiert en principe une autorisation préalable sauf exceptions. Il n'apparait toutefois pas avec clarté si cette interprétation est générale ou intrinsèquement liée à la situation d'espèce. En effet, selon ses termes : « la Cour constate que, en ce qui concerne l'accès au contenu d'un ordinateur personnel par la police, la jurisprudence du Tribunal constitutionnel a établi la règle de l'autorisation judiciaire préalable, condition exigée en tout état de cause par l'article 8 de la Convention (qui requiert la délivrance d'un mandat par un organe indépendant) lorsqu'une atteinte à la vie privée d'une personne est en jeu. La jurisprudence constitutionnelle espagnole permet toutefois, à titre exceptionnel, de passer outre une telle autorisation dans des situations d'urgence ("nécessité urgente") pouvant faire l'objet d'un contrôle judiciaire postérieur »[1298]. L'usage de « en tout état de cause » nous permet de penser que l'exigence d'une autorisation préalable par un organe indépendant dans le cadre d'une saisie dépasse la portée de cet arrêt. Quoi qu'il en soit, le contrôle postérieur en cas d'urgence doit permettre de vérifier la présence des raisons pour lesquelles l'attente de cette autorisation risque d'entraver le bon déroulement de l'enquête. En l'espèce, les services de police avaient consulté les données contenues dans un ordinateur portable qui leur avait été remis. La Cour considère cette urgence difficilement justifiable puisque la consultation de données informatiques visait les archives d'un système entre les mains des autorités et par ailleurs déconnecté d'internet de sorte qu'une autorisation aurait pu être demandée en temps utile.

3. L'observation

284. Principe. L'article 47*sexies* du Code d'instruction criminelle régit « l'observation systématique, par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés ». Est notamment considérée comme systématique, l'observation « dans le cadre de laquelle des moyens techniques sont utilisés »[1299] ou une observation de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois. Une telle mesure est strictement encadrée : elle peut être mise en œuvre par les services de police après autorisation du procureur du Roi, dans le cadre de l'information, si les nécessités de l'enquête l'exigent et si d'autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité. De surcroît, une observation effectuée à l'aide de moyens techniques ne peut être autorisée que lorsqu'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde. Enfin, lorsque l'observation systématique est utilisée pour entamer une enquête proactive[1300], on notera qu'est requise l'autorisation écrite et préalable du procureur du Roi.

1297 Cour eur. D.H., 30 mai 2017, *Trabajo Rueda c. Espagne*, n° 32600/12, § 35.

1298 *Ibid.*

1299 Selon l'article 47*sexies* du Code d'instruction criminelle est un moyen technique « une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception des moyens techniques utilisés en vue de l'exécution d'une mesure visée à l'article 90*ter* ».

1300 Selon l'article 28*bis* du Code d'instruction criminelle, « Celle-ci, dans le but de permettre la poursuite d'auteurs d'infractions, consiste en la recherche, la collecte, l'enregistrement et le traitement de données et d'informations sur la base d'une suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas

285. L'observation systématique et la vidéosurveillance. Selon la Cour de cassation, ne constitue pas une méthode particulière de recherche au sens de l'article 47*sexies* du Code d'instruction criminelle, le fait d'utiliser les informations obtenues par un moyen technique dont dispose un tiers qui met à disposition de la police les données collectées. Dès lors, en l'espèce, le visionnage *a posteriori* par les services de police d'une caméra de surveillance placée par la ville de Charleroi afin de pouvoir identifier un véhicule impliqué dans un accident ne constitue pas une observation systématique[1301].

286. Le patrouillage sur internet et l'observation systématique. En vertu de l'article 26 de la loi sur la fonction de police, les officiers de police judiciaire peuvent toujours pénétrer dans les lieux qui leur sont légalement accessibles[1302], c'est-à-dire notamment *les lieux accessibles au public*[1303], en vue de rechercher les crimes, les délits et les contraventions, d'en rassembler les preuves et d'en livrer les auteurs aux tribunaux chargés de les punir[1304]. Aucune disposition similaire n'est prévue dans un contexte digital. Dans un arrêt du 28 mars 2017, la Cour de cassation dit pour droit que l'article 26 de la loi sur la fonction de police constitue une base légale suffisante pour permettre aux services de police judiciaire d'enquêter sur internet et ses espaces « accessibles au public »[1305].

En l'espèce, des enquêteurs avaient dû installer le navigateur Tor Browser, navigateur permettant d'assurer – en théorie, l'anonymat des utilisateurs du réseau Tor afin d'accéder au darknet[1306]. Puis, après avoir effectué une recherche permettant d'obtenir un lien d'invitation généré automatiquement sur un site répertoriant différentes places de marché en ligne du darknet, ils avaient pu s'enregistrer sur l'une d'elles (Agora) sous le couvert de l'alias « Happy Holland » et observer des comportements délinquants sur ce site. Sur la base du profil d'un des utilisateurs et de ses commentaires, celui-ci fut poursuivi et finalement condamné par la cour d'appel d'Anvers pour le trafic d'amphétamines (speed) et de MDMA/MDEA (XTC). En cassation, le demandeur contestait la recevabilité des preuves recueillies sur Agora. Selon ce dernier, cette place de marché en ligne devait être considérée comme un « lieu privé » ou un « club virtuel » accessible à un nombre limité de personnes en raison des modalités d'inscription. En conséquence, les enquêteurs auraient dû obtenir l'ordonnance d'un juge d'instruction conformément aux dispositions relatives à la recherche dans un système informatique[1307] ou, à tout le moins, même à considérer qu'il n'y avait

encore connus, et qui sont ou seraient commis dans le cadre d'une organisation criminelle, telle que définie par la loi, ou constituent ou constitueraient un crime ou un délit tel que visé à l'article 90*ter*, §§ 2, 3 et 4 ».

1301 Cass., 16 mars 2016, R.G. n° P.15.1602.F, *Lar. Cass.*, 2016/10, p. 229 ; Cass., 16 mars 2016, P.15.1602.F, *Rev. dr. pén.*, 2017/5, pp. 482-492.

1302 Art. 26 de la loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992.

1303 M. Franchimont, A. Jacobs, A. Masset, « § 8. – Les perquisitions (art. 87 et 88 C.I.C.) », in *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, pp. 515-531.

1304 Art. 8 CICr.

1305 Cass., 28 mars 2017, R.G. n° P.16.1245.N/4.

1306 Un réseau de type « darknet » permet en théorie de rester anonyme puisqu'il n'implique pas un partage public des adresses IP.

1307 Il s'agissait de l'article 88*ter* du Code d'instruction criminelle (ci-après CICr). Cette disposition est à présent inclue dans l'article 39*bis* CICr suite à l'adoption de la 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.

pas eu d'intrusion dans son compte privé, les enquêteurs auraient dû respecter les dispositions relatives au contrôle visuel discret ou l'observation systématique[1308].

La Cour de cassation rejeta l'argument et considéra qu'Agora ne pouvait être qualifiée « d'espace non accessible au public ». En effet, selon la Cour, l'accès à ce site dépendait de conditions purement formelles, « sans contrôle réel ou sans vérification sur la qualité des personnes ». Dès lors, les utilisateurs ne pouvaient « s'attendre raisonnablement » à ce que cet espace soit limité à un cercle privé. De plus, les enquêteurs n'avaient pas adopté une identité fictive crédible ou utilisé un alias provocant ou encore, fait usage d'un mot de passe, d'un login ou de clés de chiffrement afin de « craquer » l'accès au système informatique. Appliquant par analogie les méthodes d'enquête dans un contexte réel au contexte digital, la Cour rappela qu'en vertu de l'article 26 de la loi sur la fonction de police, les officiers de police judiciaire peuvent toujours pénétrer dans les lieux qui leur sont légalement accessibles[1309], c'est-à-dire notamment *les lieux accessibles au public*[1310]. Dès lors, *in casu*, les services de police n'avaient pas outrepassé leurs compétences de police judiciaire.

4. Les différentes obligations de collaboration dans un contexte informatique

a. La rétention de données[1311]

287. Principes. L'obligation de conservation généralisée des « métadonnées »[1312] imposée aux opérateurs et fournisseurs de réseaux et services de communications électroniques est controversée[1313]. La mesure consiste, en effet, en la collecte et le stockage systématique et *a priori* de l'ensemble des données traitées et générées lors d'une communication électronique à l'exception du contenu de celle-ci. Elle implique donc une ingérence « particulièrement grave » dans le droit au respect de la vie privée et à la protection des données à caractère personnel[1314].

288. Première épisode : l'arrêt *Digital Rights* de la C.J.U.E. Au niveau européen, la directive 2006/24/CE[1315] a été déclarée « invalide » le 8 avril 2014 par la Cour de justice de l'Union européenne en raison de l'absence de garanties suffisantes permettant de limiter l'ingérence « au strict nécessaire »[1316]. Premièrement, elle fit le constat du caractère généralisé du dispositif en cause, les données étant collectées de manière globale indépendamment d'un lien entre l'attitude des personnes et des éventuelles infractions graves[1317]. Deuxièmement, elle pointa l'absence d'un cadre procédural ou matériel permettant de limiter l'accès aux données collectées ou l'utilisa-

1308 Art. 46*quinquies*, 47*sexies*, 56*bis* et 89*ter* CICr.

1309 Art. 26 de la loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992.

1310 M. Franchimont, A. Jacobs, A. Masset, « § 8. – Les perquisitions (art. 87 et 88 C.I.C.) », in *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, pp. 515-531.

1311 Au sujet de cette problématique, voy. également les n^{os} 152 et 153 de la présente chronique.

1312 Les « métadonnées » sont les données traitées et générées lors d'une communication électronique à l'exception du contenu de celle-ci.

1313 Pour une analyse, voy. C. Forget, « L'obligation de conservation des "métadonnées" : la fin d'une longue saga juridique ? », *J.T.*, 2017/13, n° 6683, pp. 233-239 ; M. Panzavolta, S. Royer et H. Severijns, « Algemene dataretentie: ten minste houdbaar tot…? », *T. Strafr.*, 2018, afl. 1, pp. 2-16.

1314 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, aff. C-293/12 et C-594/12.

1315 Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, *J.O.U.E.* L 105 du 13 avril 2006, pp. 54-63, (ci-après directive 2006/24/CE).

1316 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, aff. C-293/12 et C-594/12.

1317 Point 58 de l'arrêt *Digital Rights*.

tion de celles-ci par les autorités nationales[1318]. Troisièmement, la Cour souligna au sujet de la durée de conservation de six à vingt-quatre mois l'absence de lien entre les différentes catégories de données collectées et l'objectif poursuivi[1319]. Elle conclut que l'ingérence était donc « d'une vaste ampleur et d'une gravité particulière » sans être « précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire »[1320].

289. L'annulation de la loi du 30 juillet 2013 par la Cour constitutionnelle. Sur la base de l'arrêt *Digital Rights*, la Cour constitutionnelle annule avec effet rétroactif la loi du 30 juillet 2013 transposant la directive 2006/24/CE dans l'ordre interne[1321]. Alignant son argumentaire sur celui de la Cour de justice de l'Union européenne, la Cour conclut que « par identité des motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive conservation des données invalide »[1322], le législateur national a dépassé les limites qu'impose le respect du principe de proportionnalité[1323]. Ce raisonnement pour le moins rapide, appelle plusieurs observations. Premièrement, la Cour constitutionnelle a omis de tenir compte de différences essentielles entre la directive 2006/24/CE et la loi du 30 juillet 2013. À la différence de la directive, la loi attaquée encadrait l'accès aux données puisqu'elle se référait aux articles 46*bis* et 88*bis* du Code d'instruction criminelle et à la loi du 30 novembre 1998 relative aux services de renseignements et de sécurité. Deuxièmement, la Cour constitutionnelle examina la légalité de la loi du 30 juillet 2013 sans prendre en considération la disparition de la directive 2006/24/CE de l'ordre juridique européen. Or, une fois cette norme européenne invalidée, la disposition nationale aurait dû être examinée au regard des critères établis par l'article 15, § 1, de la directive 2002/58/CE en combinaison avec les articles 7, 8 et 52, § 1, de la Charte.

290. Recevabilité des preuves. Une violation de l'article 8 de la CEDH garantissant le droit au respect de la vie privée n'entraîne pas *ipso facto* une violation de l'article 6 de la CEDH, consacrant le droit au procès équitable. En effet, il ressort de l'article 32 du titre préliminaire du Code pénal que : « La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si : le respect des conditions formelles concernées est prescrit à peine de nullité, ou l'irrégularité commise a entaché la fiabilité de la preuve, ou encore l'usage de la preuve est contraire au droit à un procès équitable ». Dès lors, les données conservées et accessibles aux enquêteurs sur la base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques tel que modifié par la loi du 30 juillet 2013 malgré l'annulation de cette disposition par la Cour constitutionnelle, ne sont pas *ipso facto* irrégulières ou inadmissibles à titre de preuve. La Cour de cassation considère que l'article 88*bis* du Code d'instruction criminelle, à savoir le repérage, constitue une base légale suffisante pour l'utilisation de ces données. De plus, ces données ne pourraient être écartées en vertu de l'article 32 du titre préliminaire du Code pénal dans la mesure où il n'y a ni violation

1318 Point 60 de l'arrêt *Digital Rights*.
1319 Point 63 de l'arrêt *Digital Rights*.
1320 Point 65 de l'arrêt *Digital Rights*.
1321 C. const., 11 juin 2015, n° 84/2015.
1322 C. const., 11 juin 2015, n° 84/2015, point B.11.; C. Conings et F. Verbruggen, « Grondwettelijk Hof plaatst reparateurs dataretentiewet voor moeilijke opdracht », *Juristenkrant*, 2015, afl. 312, pp. 1 et 3.
1323 C. const., 11 juin 2015, n° 84/2015, point B.10.1.

de forme prescrite à peine de nullité ni atteinte à la fiabilité de la preuve et l'utilisation de ces données n'emporte aucune atteinte irréversible aux droits de la défense[1324].

291. Deuxième épisode : l'arrêt *Tele2* de la C.J.U.E. L'arrêt *Tele2* récemment rendu par la Cour de justice fait suite à deux questions préjudicielles posées par les juridictions suédoise et britannique[1325]. Celles-ci s'interrogent sur la compatibilité au droit de l'Union d'une réglementation nationale imposant la conservation de données telle que le prévoyait la directive 2006/24/CE[1326]. Ce faisant, la Cour est amenée à préciser la portée de l'arrêt *Digital Rights* et elle a ainsi l'occasion de préciser les conditions d'une conservation de données indépendamment des conditions d'accès à ces données par les autorités compétentes. Concernant la conservation, la Cour de justice censure une obligation de conservation de données imposée aux opérateurs en raison de son caractère « généralisé et indifférencié » et préconise une conservation « ciblée » des métadonnées. En effet, selon la Cour, l'article 15, § 1, de la directive 2002/58/CE ne s'oppose pas à une « réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave » mais dans le respect de certaines conditions[1327]. En premier lieu, le texte doit contenir des garanties suffisantes, c'est-à-dire une réglementation claire, accessible et prévisible permettant d'éviter tout risque d'abus et de protéger efficacement les données à caractère personnel[1328]. En second lieu, des conditions matérielles relatives à la conservation des données doivent établir « un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné »[1329]. Et la Cour de préciser ce qu'elle entend par « public et situations potentiellement concernées », à savoir qu'il s'agit de fixer dans la réglementation « des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique »[1330].

292. Dernier épisode ? L'arrêt rétention *bis* de la Cour constitutionnelle. Suite à l'arrêt de la Cour constitutionnelle du 11 juin 2015, le législateur s'est empressé d'adopter la loi du 29 mai 2016[1331] afin de combler le vide juridique laissé tout en intégrant, dans la mesure du possible, les critiques adressées par la Cour de justice et par la Cour constitutionnelle[1332]. Toutefois depuis l'arrêt *Tele2*, il paraît difficile d'affirmer que la loi du 29 mai 2016 rencontre les exigences formulées par la C.J.U.E. alors que celle-ci condamne clairement la conservation « générale et indifférenciée »

1324 Cass., 19 avril 2016, *T. Strafr.*, 2016/5, pp. 366-368.

1325 C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB et Secretary of State for the Home Department*, aff. C-203/15 et C-698/15.

1326 En particulier, la Cour effectue son examen au regard de l'article 15, § 1, de la directive 2002/58/CE pris à la lumière des articles 7, 8, 11 et 52, § 1, de la Charte des droits fondamentaux de l'Union européenne.

1327 Point 108 de l'arrêt *Tele2*.

1328 Point 109 de l'arrêt *Tele2*. La Cour ajoute que le texte doit donc « indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise ». Ce critère est également rappelé à de nombreuses reprises par la Cour européenne des droits de l'homme. Voy. entre autres Cour eur. D.H., 2 août 1984, *Malone c. Royaume-Uni*, série A n° 82, § 67.

1329 Point 110 de l'arrêt *Tele2*.

1330 Point 111 de l'arrêt *Tele2*.

1331 Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016.

1332 *Doc. parl.*, Ch. repr., 2015-2016, n° 54-1567/001, p. 76.

de données indépendamment des conditions d'accès. En effet, les améliorations apportées par le législateur national[1333] ne sauraient suffire à respecter les exigences d'une collecte « ciblée » des données, exigences qui imposent de fixer dans la réglementation l'ampleur de la mesure et le public concerné en fonction de l'objectif poursuivi. Quoi qu'il en soit, la balle est à présent dans le camp de la Cour constitutionnelle puisque l'Ordre des barreaux francophones et germanophone et les ASBL Liga voor Mensenrechten et Ligue des Droits de l'Homme ont introduit des recours en annulation à l'encontre de la loi du 29 mai 2016.

b. L'identification

293. Principe. Le procureur du Roi peut solliciter le concours des opérateurs et fournisseurs de communications électroniques afin de procéder à l'identification d'un utilisateur de ses services en obtenant, par exemple, les informations relatives à une ligne téléphonique, une adresse de courrier électronique, une adresse IP, un code IMEI d'un téléphone[1334] ou encore l'adresse MAC d'un ordinateur[1335]. Dans le cas où l'infraction n'est pas de nature à emporter une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut accéder qu'aux données d'indentification conservées depuis six mois à partir de sa décision[1336]. Ces données doivent être fournies sur demande « en temps réel » sous peine d'une amende de vingt-six euros à dix mille euros en cas de refus ou d'absence de réaction[1337]. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel[1338].

294. La notion de fournisseur de communications électroniques. L'affaire « *Yahoo!* » fait suite au refus de l'entreprise de prêter son concours considérant qu'elle ne pouvait être qualifiée de « fournisseurs de service de communications électroniques » eu égard à la loi du 13 juin 2005 sur les communications électroniques. En 2011, la Cour de cassation considéra cependant devoir interpréter la notion de « fournisseur d'un service de communications électroniques » de manière autonome par rapport à la loi du 13 juin 2005 et imposa dès lors à la société de fournir les données requises[1339]. Cette approche fut également retenue par le tribunal correctionnel de

1333 En vertu de l'article 126, § 3, de la loi du 13 juin 2005 tel que modifié par la loi du 29 mai 2016, les données sont catégorisées mais conservées durant une période unique de douze mois et ce, indépendamment de leur intérêt potentiel dans le cadre d'enquêtes pénales. De plus, la mesure présente toujours le risque d'atteinte au secret professionnel, les données des avocats et des médecins étant stockées indépendamment de leur caractère confidentiel. Notons que la proposition initiale suggérait de conserver les données d'identification durant douze mois. Les données de connexion et de localisation devaient être conservées entre neuf et douze mois. Seules les données de communication devaient être conservées 2 mois. En définitive, plus les données sont potentiellement utiles pour les enquêteurs, plus la durée de conservation aurait été longue. *Doc. parl.*, Ch. repr., 2015-2016, n° 54-1567/001, p. 11.

1334 International Mobile Equipment Identity. L'IMEI est un numéro permettant d'identifier de manière unique les terminaux d'un téléphone mobile. Toute personne peut l'obtenir en composant le code : « *#06# » sur le clavier de son téléphone portable.

1335 L'adresse MAC est un identifiant stocké dans une carte réseau ou une interface réseau stockée dans l'ordinateur. Elle permet de se connecter au routeur d'un réseau.

1336 Art. 46*bis*, § 1, dernier alinéa, CICr.

1337 Art. 46*bis*, § 2, dernier alinéa, CICr.

1338 Art. 46*bis*, § 2, al. 3, CICr.

1339 Cass., 18 janvier 2011, *N. C.*, 2011/1, pp. 76-85. Pour une analyse, voy. K. De Schepper et F. Verbruggen, « Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners », *T. Straf.*, 2013, pp. 143-166.

Malines et confirmée par la cour d'appel d'Anvers, à l'égard de Skype, estimant que ce dernier devait collaborer dans les conditions prévues par les articles 88*bis*, § 2, et 90*quater*, § 2, CICr en tant que fournisseurs de services de communications électroniques[1340]. Cette interprétation fut entérinée par la loi du 25 décembre 2016 élargissant le spectre des tiers tenus à collaborer dans le cadre d'une demande d'identification, de repérage ou d'interception des communications[1341].

295. La compétence territoriale des juridictions dans le cadre d'une mesure d'identification. L'affaire « *Yahoo!* » est remontée une troisième fois devant la Cour de cassation en 2015. Le procureur du Roi avait pris une sanction pénale sur la base de l'article 46*bis*, § 1, alinéa 4, CICr, l'entreprise refusant toujours de prêter son concours[1342]. La Cour de cassation dut estimer si la cour d'appel d'Anvers n'avait pas outrepassé sa compétence territoriale compte tenu du lieu d'établissement de l'entreprise. La Cour dit pour droit que l'infraction prévue à l'article 46*bis*, § 2, alinéa 4, du Code d'instruction criminelle est commise à l'endroit où les données requises doivent être reçues. Par conséquent, l'opérateur ou le fournisseur qui refuse de communiquer ces données est passible d'une peine en Belgique, quel que soit le lieu où il est établi. La Cour en déduit, d'une part, que la mesure consistant en l'obligation de fournir les données visées en l'espèce est prise sur le territoire belge à l'égard de chaque opérateur ou fournisseur qui oriente activement ses activités économiques vers des consommateurs en Belgique et, d'autre part, que la juridiction belge qui condamne un opérateur ou fournisseur établi à l'étranger en raison de l'inobservation de cette obligation et impose ainsi le respect d'une mesure prise en Belgique, n'exerce pas de pouvoir de juridiction extraterritorial.

c. Le dispositif « Passenger Name Records »

296. L'accord PNR UE/Canada. Le 23 juin 2014, le Canada et le Conseil de l'UE signaient un accord en vertu duquel les données « PNR »[1343] sont systématiquement transmises à l'Agence des services frontaliers de ce pays tiers en vue d'évaluer les risques potentiels que les passagers aériens pourraient présenter pour la sécurité publique[1344]. En dépit des réserves émises par le

1340 Corr. Anvers, 27 octobre 2016, *NjW*, 2016/20, pp. 921-928. Pour un commentaire, voy. J. Flo, « Skype moet onderzoekers toegang geven tot communicatie verdachte », *Juristenkrant*, n° 337. Cette approche fut confirmée par la cour d'appel d'Anvers (Anvers, 15 novembre 2017, R.G. n° C.1288.2017, inédit. Voy. J. Flo, « Skype opnieuw veroordeeld voor belemmering strafonderzoek », *Juristenkrant*, 2017, n° 359).

1341 Art. 46*bis*, § 1, al. 3, art. 88*bis*, § 1, al. 2, et art. 90*quater*, § 2, CICr.

1342 Cass., 1er décembre 2015, R.G. n° P.13.2082.N, *Pas.*, 2015/13, pp. 92-94 ; K. De Schepper, « Cassatie bevestigt: Belgische gerecht kan rechtstreeks gegevens vorderen van Yahoo », *R.A.B.G.*, 2016/7, pp. 489-493 ; P. Vandenbruwaene, « Uitdagingen voor de rechtshandhaving in cyberspace », *R.W.*, 2016-2017, liv. 20, pp. 763-777.

1343 Les données PNR sont les informations initialement collectées par les transporteurs aériens à des fins commerciales. Il s'agit notamment de l'itinéraire complet, l'agence de voyage, le numéro de siège, les informations relatives aux bagages, les données d'enregistrement et d'embarquement (type de document de voyage, numéro du document, nationalité, nombre, poids et identification des bagages, numéro de transport, etc.), les modes de paiement, et de manière large, des remarques générales à l'égard de chaque passager.

1344 La particularité du système PNR est l'exploration systématique de données afin de « situer » des passagers sur une échelle de risques et d'ainsi permettre l'identification de criminels « éventuels ou probables ». Selon le Conseil de l'Europe, un tel mécanisme ciblant des personnes « qui n'ont commis aucune infraction » ne pourrait en aucun cas viser « un but légitime » d'autant qu'il existe un risque d'erreur inévitable susceptible de mener à du profilage discriminatoire. Voy. en ce sens le rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, *Passenger Name Records, data mining & data protection: the need for strong safeguards*, 15 juin 2015, T-PD(2015)11.

Groupe Article 29[1345] et le Contrôleur européen de la protection des données[1346], le texte fut soumis pour approbation au Parlement en juillet 2014. Le Parlement s'interrogea, d'une part, sur la finalité de l'accord et, d'autre part, sur les garanties nécessaires pour garantir une ingérence légale et proportionnée dans les droits à la vie privée et à la protection des données à caractère personnel. Dans l'esprit du traité de Lisbonne, le Parlement saisit la Cour de justice de l'Union européenne d'une demande d'avis.

297. L'avis de la C.J.U.E. Dans un avis du 26 juillet 2017[1347], la Cour de justice de l'Union européenne affirme le caractère généralisé et indifférencié du transfert des données PNR tout en estimant que celui-ci « facilite et accélère grandement les contrôles de sécurité et les contrôles aux frontières »[1348]. La Cour dresse à la lumière de sa jurisprudence antérieure[1349], une liste de points devant être revus, à savoir : la clarification des catégories de données transférées[1350], l'exclusion du traitement des données sensibles en raison de l'absence de justification précise et solide[1351], l'utilisation de modèles et critères préétablis spécifiques, fiables et non discriminatoires[1352], la limitation du recoupement de données avec d'autres bases de données présentant un lien avec le but visé[1353], l'exclusion des finalités vagues et générales[1354], la période de conservation de données en rapport avec l'objectif poursuivi[1355], l'accès aux données basé sur une demande motivée des autorités compétentes répondant à des critères objectifs[1356] couplé à un contrôle préalable par une juridiction ou une entité administrative indépendante[1357], la communication des données PNR à un pays tiers sous réserve d'un accord entre l'Union et ce pays tiers équivalent à l'accord envisagé ou d'une décision d'adéquation de la Commission[1358], l'existence des droits des personnes concernées (accès, rectification, information individuelle)[1359], le droit à un recours effectif[1360] et enfin le contrôle du respect de ces règles par une autorité de contrôle indépendante[1361]. Selon la Cour, sous réserve du respect de l'ensemble de ces conditions, l'accord envisagé rencontrerait les exigences de la Charte des droits fondamentaux.

1345 Groupe Article 29, avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, adopté le 12 novembre 2010.

1346 CEPD, avis du 15 juin 2005 sur la proposition de décision du Conseil relative à la conclusion d'un accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations anticipées sur les voyageurs (API)/dossiers passagers (PNR), *J.O.C.E.* C 218 du 6 septembre 2005, p. 6 ; CEPD, avis du 30 septembre 2013 sur les propositions de décisions du Conseil relatives à la conclusion et à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers.

1347 C.J.U.E., 26 juillet 2017, avis 01/2015, *J.O.C.E.* C 51 du 22 février 2014, p. 12 (ci-après, avis).

1348 Point 151 de l'avis.

1349 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, aff. C-293/12 et C-594/12 ; C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15 ; C.J.U.E., 6 octobre 2015, *Schrems*, aff. C-362/14.

1350 Point 163 de l'avis.

1351 Point 165 de l'avis.

1352 Point 174 de l'avis.

1353 *Ibid.*

1354 Point 181 de l'avis.

1355 Points 190 à 203 de l'avis.

1356 Point 200 de l'avis.

1357 Point 202 de l'avis.

1358 Point 214 de l'avis.

1359 Point 221 de l'avis.

1360 Point 227 de l'avis.

1361 Point 230 de l'avis.

298. La communication des données des passagers en droit belge. La loi du 25 décembre 2016 relative au traitement des données des passagers[1362] transpose partiellement la directive PNR[1363] et introduit une obligation pour les transporteurs et opérateurs de voyage des différents secteurs de transport international (aérien, ferroviaire, routier et maritime) de transmettre les informations relatives à leurs passagers[1364] à une banque de données gérée par le Service public fédéral Intérieur[1365]. Ces données ont vocation à être analysées avant l'arrivée, le transit ou le départ d'une personne sur le territoire national[1366] par l'Unité d'Informations des Passagers (UIP) créée au sein du SPF Intérieur[1367]. Cette méthode appliquée à des fins de « pre-screening »[1368] permettrait de « faire émerger des profils de passagers à risque qui ne sont pas nécessairement connus ou mentionnés dans les banques de données des services »[1369]. En outre, les services compétents[1370] ont la possibilité de procéder à des recherches ponctuelles dans les limites de leurs missions et des finalités prévues par la loi, à savoir notamment la lutte contre le terrorisme, la recherche et la poursuite de certaines infractions et la lutte contre l'immigration illégale[1371]. Conformément à l'article 46*septies* CICr, le procureur du Roi peut, sur la base d'une décision écrite et motivée, charger l'officier de police judiciaire de requérir l'UIP afin d'obtenir la communication de données de passagers. Toutefois, l'article 46*septies*, § 2, CICr impose le respect des critères de proportionnalité et de subsidiarité par rapport à d'autres devoirs d'enquête. Si la demande porte sur un ensemble de données relatives à une enquête spécifique, celle-ci doit alors être limitée à une période d'un mois, sans préjudice de renouvellement[1372]. Notons toutefois que l'avis « PNR » précité aura probablement des conséquences sur notre législation nationale d'autant qu'un recours en annulation est actuellement pendant devant la Cour constitutionnelle[1373].

1362 Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017.

1363 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) 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, *J.O.U.E.* L 119 du 4 mai 2016, pp. 132-149 (ci-après directive PNR).

1364 L'article 9 de la loi PNR distingue les données API, à savoir les données d'enregistrement et d'embarquement, des données PNR, à savoir les données de réservation. Les données API sont des données authentiques, par exemple, données biographiques figurant sur une carte d'identité. Les données PNR comprennent davantage d'informations. Il s'agit notamment de l'itinéraire complet pour le passager, l'agence de voyage, le numéro de siège, les informations relatives aux bagages, les données d'enregistrement et d'embarquement (type de document de voyage, numéro du document, nationalité, nombre, poids et identification des bagages, numéro de transport, etc.), les modes de paiement et l'adresse de facturation, etc.

1365 Art. 3 loi PNR.

1366 Art. 15 loi PNR.

1367 Art. 24 loi PNR.

1368 Le « pre-screening » consiste en « l'évaluation du risque représenté par les passagers » et s'effectue par le biais d'une corrélation entre les banques de données des services compétents ou par le biais de critères préétablis par l'UIP.

1369 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-2069/001, p. 29.

1370 Par « services compétents », l'article 14, § 1, 2°, précise qu'il s'agit des services de police, de la Sûreté de l'État, du Service général de Renseignement et de Sécurité, de services d'enquêtes liées aux infractions douanes et accises.

1371 Art. 8 loi PNR.

1372 Art. 46*septies*, § 3, CICr.

1373 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 ».

d. L'obligation de collaboration

299. Principe. L'article 88*quater* du Code d'instruction criminelle prévoit deux types de demandes de collaboration relevant de la compétence du juge d'instruction. La première est une obligation d'information qui peut être imposée à quiconque est présumé disposer d'une connaissance particulière du système informatique faisant l'objet d'une recherche ou de son extension, de fournir, dans une forme compréhensible, des informations sur le fonctionnement de ce système[1374]. Un tiers pourrait, par exemple, être forcé de fournir les clés de chiffrement ou les mots de passe dont il aurait connaissance, sur demande des autorités. La seconde est une obligation « d'agir » dans le sens où le juge d'instruction peut ordonner à toute personne appropriée de mettre ledit système en fonctionnement et de copier les données, de les rendre inaccessibles ou encore de les retirer de l'appareil exploité[1375]. On précisera que la mesure ne peut porter atteinte au droit au silence et aux règles de droit commun relatives aux personnes tenues au secret professionnel[1376]. Sous réserve de ces exceptions, le défaut de collaboration est passible de sanctions pénales[1377].

300. L'interdiction d'obliger un suspect à collaborer activement avec les autorités poursuivantes. Dans un arrêt du 23 juin 2015[1378], la cour d'appel de Gand a rappelé le « droit au silence » impliquant qu'aucun suspect ne peut être obligé de collaborer activement avec les autorités poursuivantes. Elle estime qu'en ordonnant aux prévenus de rendre accessibles les supports de données, ils avaient été contraints, moyennant une prestation intellectuelle propre, de contribuer activement à l'administration de la preuve de sorte que les éléments de preuve fournis par les supports de données cryptées étaient frappés de nullité.

301. Le mot de passe d'un téléphone et le champ d'application du droit au silence. Récemment toutefois, la cour d'appel d'Anvers, chambre des mises en accusation, a considéré que l'ordonnance d'un juge d'instruction imposant à un inculpé de dévoiler le code PIN de son téléphone portable sous peine de sanctions pénales afin de permettre aux enquêteurs d'exploiter les données stockées, n'était pas incompatible avec les exigences du droit à un procès équitable[1379]. Dans sa décision, la chambre des mises en accusation a notamment fait référence à l'arrêt *Saunders* où la Cour eur. D.H. a estimé qu'une donnée que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existe indépendamment de sa volonté, tels des documents recueillis sur la base d'un mandat, des empreintes ADN, haleine, sang, urine, n'entrait pas dans le champ d'application du droit au silence[1380]. Cette interprétation mérite d'être nuancée puisqu'à la différence de documents fiscaux par exemple, établis en vertu d'une obligation légale et saisissables dans le cadre d'une perquisition, un mot de passe est en principe créé sur initiative de

1374 Art. 88*quater*, § 1, CICr.
1375 Art. 88*quater*, § 2, CICr.
1376 *Doc. parl.*, Ch. repr., 1999-2000, n° 0213/001, p. 28. Voy. à cet égard la jurisprudence de la Cour constitutionnelle : C. const., 17 décembre 2015, n° 178/2015, B.52.3 ; J. Coppens et C. Van De Heyning, « Het bevel tot medewerking van artikel 88*quater* Sv., het zwijgrecht en het verbod op zelfincriminatie », *T.S.*, n° 3, 2016, pp. 260-265.
1377 Art. 88*quater*, § 3, al. 1, CICr.
1378 Gand, 23 juin 2015, *NjW*, 2016, liv. 336, p. 134, note C. Conings.
1379 Anvers, 21 décembre 2017, chambre des mises en accusation, K/2895/2017, inédit.
1380 Cour eur. D.H., 17 décembre 1996, *Saunders c. Royaume-Uni*, n° 1187/91, § 69.

son auteur et devrait donc être couvert par le droit au silence[1381]. En effet, le droit au silence ne couvre pas uniquement le droit de se taire mais englobe également le droit de ne pas fournir des informations susceptibles d'affecter substantiellement la position de l'accusé ou de favoriser une incrimination[1382], ce qui pourrait être le cas lorsqu'un suspect est tenu de donner accès aux données stockées sur son téléphone.

302. La collaboration d'un tiers et le respect de l'anonymat sur internet. Dans un arrêt du 15 septembre 2016, la Cour de justice de l'Union européenne a estimé que le droit européen ne s'oppose pas à l'adoption d'une injonction judiciaire consistant à exiger d'un fournisseur d'accès à un réseau accessible au public de sécuriser la connexion à internet au moyen d'un mot de passe afin que les utilisateurs de ce réseau soient obligés de révéler leur identité et ne puissent donc pas agir anonymement[1383]. En effet, insistons sur le fait que l'anonymat est loin d'être un droit absolu et que les États ont l'obligation positive, inhérente à l'article 8 de la CEDH, d'adopter des dispositions en matière pénale qui sanctionnent effectivement les infractions contre les personnes. Dans l'arrêt *K.U. c. Finlande*, la Cour a ainsi estimé qu'une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier l'auteur[1384].

303. La collaboration de tiers dans le cadre d'une interception des communications. La collaboration de tiers en vue d'une interception des communications se fait souvent sur une base volontaire mais peut également être exigée sur la base d'une ordonnance du juge d'instruction prise en vertu des articles 88*bis* CICr et 90*quater* CICr[1385]. Le refus de collaboration « en temps réel »[1386] et le refus de prêter son concours technique sont passibles de sanctions pénales[1387]. En l'espèce, Skype devait collaborer en vue de permettre l'interception des données de communications électroniques[1388]. L'entreprise invoquait l'impossibilité matérielle de prêter son concours en raison du chiffrement des données depuis le destinateur et le déchiffrement de ces données une fois chez le destinataire. Néanmoins, selon la cour d'appel, en créant ses services, Skype aurait dû tenir compte des obligations de collaboration découlant du droit national belge. En effet, à la différence de l'article 88*quater*, § 2, CICr imposant une obligation de collaboration dans la limite des moyens dont dispose un tiers, l'article 90*quater* CICr ne prévoit aucune dérogation à l'obligation de collaboration. Ce faisant, la cour déduit de l'article 90*quater* CICr une obligation positive à charge des tiers dès la conception d'application. Cette obligation peut sembler entrer

1381 Cour eur. D.H., 25 février 1993, *Funke c. France*, n° 110588/83.

1382 Cour eur. D.H., 19 février 2009, *Chabelnik c. Ukraine*, n° 16404/03.

1383 C.J.U.E, 15 septembre 2016, *Tobias Mc Fadden / Sony Music Entertainment Germany GmbH*, aff. C-484/14, § 102.

1384 Cour eur. D.H., 2 décembre 2008, *K.U. c. Finlande*, req. n° 2872/02, § 49. Dans cette affaire, le requérant se plaignait qu'une annonce à caractère sexuel ait été publiée à son sujet sur un site de rencontres par internet et que la législation finlandaise en vigueur à l'époque n'ait pas permis à la police et aux tribunaux d'obliger le fournisseur d'accès à identifier l'auteur de l'annonce.

1385 Afin de pouvoir intercepter les communications, le juge d'instruction peut requérir directement ou par l'intermédiaire du service de police désigné par le Roi, le concours « en temps réel » de toute personne présumée disposer de connaissance particulière du système informatique qu'elles fournissent des informations sur le fonctionnement de ce moyen ou système et sur la manière d'accéder à son contenu qui est ou a été transmis, dans une forme compréhensible. Il peut ordonner aux personnes de rendre accessible ce contenu, dans la forme qu'il souhaite, notamment dans le cas où celui-ci est chiffré. Art. 90*quater*, § 4, CICr.

1386 Art. 90*quater*, § 2, al. 4, CICr.

1387 Art. 90*quater*, § 4, al. 3, CICr.

1388 Anvers, 15 novembre 2017, R.G. n° C.1288.2017, inédit.

en résonnance avec les concepts de « *privacy by design* » et de « *privacy by default* » prévus par le RGPD[1389]. Ceux-ci imposent au responsable du traitement de prendre en considération, dès la conception, les mesures techniques et organisationnelles appropriées relatives à la protection des données et au respect de la vie privée[1390]. Cependant, la question mérite d'être posée quant à savoir si ces approches vont jusqu'à leur imposer des obligations de « *collaboration by design* » avec les autorités policières et judiciaires. À cet égard, le Groupe 29 a encore récemment rappelé que « *encryption must remain standardized, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys. Whatever the technical solution, it can never be safe to compel encryption providers to include master keys and backdoors in their software. Law enforcement agencies already have access to vast quantities of data via their existing powers. Such access must remain proportionate and targeted. They should focus on improving their capabilities to interpret those data to investigate and prosecute criminals* »[1391]. Dans cette mesure, l'interprétation de la cour selon laquelle l'article 90*quater* du Code d'instruction criminelle prévoit une telle obligation « positive » à charge de tiers est critiquable.

e. L'interception des communications

304. L'interdiction d'une interception généralisée du contenu des communications. L'affaire *Schrems* fait suite à une plainte de Monsieur Schrems visant à faire interdire le transfert de ses données par « Facebook Ireland » vers les États-Unis. Celui-ci, s'appuyant sur les révélations d'Edward Snowden, dénonçait l'absence de niveau de protection adéquat des données à caractère personnel sur le sol américain en dépit de la décision *Safe Harbor* de la Commission. Dans ce cadre, la Cour de justice de l'Union européenne a fermement condamné toute mesure permettant l'interception *généralisée* du contenu des communications, celle-ci impliquant une « atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte »[1392].

305. Les critères relatifs à l'interception des communications. Dans le domaine des mesures de surveillance secrète, la Cour eur. D.H. tient compte des critères suivants : « la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistre-

1389 Art. 25 du RGPD.

1390 Art. 25 du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), *J.O.U.E.* L 119 du 4 mai 2016, p. 1 (ci-après le règlement général sur la protection des données).

1391 Groupe 29, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, 11 avril 2018, p. 3.

1392 C.J.U.E. (gr. ch.), 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, aff. C-362/14. Cette affaire fait suite à une plainte de Monsieur Schrems visant à faire interdire le transfert de ses données par Facebook Ireland vers les États-Unis. Celui-ci s'appuyant sur les révélations d'Edward Snowden, dénonçait l'absence de niveau de protection adéquat des données à caractère personnel sur le sol américain en dépit de la décision *Safe Harbor* de la Commission. À ce sujet, voy. également les n^os^ 145 et 146 de la présente chronique.

ments »[1393]. Selon la Cour eur. D.H., le champ d'application de la mesure doit être déterminé avec suffisamment de précision tant concernant la nature des infractions susceptibles de donner lieu à un mandat d'interception que vis-à-vis des catégories de personnes susceptibles d'être concernées. S'agissant des infractions, la Cour eur. D.H. n'exige pas de prévoir une liste exhaustive[1394]. La mesure peut, par exemple, viser de manière large « les faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique » et ainsi, conférer aux autorités une « latitude quasi illimitée » lorsqu'il s'agit d'identifier les actes susceptibles de faire procéder à l'interception des communications[1395]. Néanmoins, la Cour eur. D.H. examine si la marge de manœuvre laissée aux autorités peut être limitée par le biais d'une autorisation judiciaire préalable par exemple[1396]. Concernant les personnes susceptibles de faire l'objet d'une mesure de surveillance, il peut s'agir d'un suspect ou d'un prévenu, mais aussi d'un individu susceptible de détenir des informations sur une infraction ou d'autres informations pertinentes pour un dossier pénal[1397].

306. L'interception des communications à grande échelle[1398]. La Cour eur. D.H. ne semble pas considérer que les mesures d'interception des communications à grande échelle emportent *ipso facto* la violation de la Convention, la Cour examinant l'ensemble des garanties offertes par la disposition soumise à son contrôle[1399] et ce, sans soumettre « les règles gouvernant l'interception de communications individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents »[1400]. À titre illustratif, dans l'arrêt *Szabo c. Hongrie*, tout en mettant l'accent sur certaines préoccupations compte tenu du risque d'ouvrir la voie à une « surveillance illimitée d'un grand nombre de citoyens », la Cour eur. D.H. affirma que le recours à des technologies de pointe, y compris le contrôle massif des communications, est une conséquence naturelle eu égard aux nouvelles formes de terrorisme[1401]. Faisant référence à son homologue localisée à Luxembourg, la C.J.U.E., elle examina néanmoins le caractère « nécessaire dans une société démocratique » d'un tel dispositif de manière « stricte » : premièrement, de manière générale au regard de l'objectif poursuivi en l'occurrence, la sauvegarde des institutions démocratiques, deuxièmement, en particulier, afin d'obtenir des renseignements dans le cadre d'une opération individuelle[1402].

1393 Cour eur. D.H. (gr. ch.), 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06, § 231.

1394 *Ibid.*, § 244.

1395 *Ibid.*, § 248. La règlementation visait en effet potentiellement toute « personne susceptible de détenir des informations sur une infraction pénale » mais aussi toute « personne susceptible de détenir des informations pertinentes pour un dossier pénal » en raison de « faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Fédération de Russie ».

1396 Cour eur. D.H. (gr. ch.), 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06, § 249.

1397 *Ibid.*, § 245.

1398 Cour eur. D.H., 12 janvier 2016, *Szabo et Vissy c. Hongrie*, n° 37138/14, § 69.

1399 *Ibid.*, § 67.

1400 Cour eur. D.H., 1er juillet 2008, *Liberty e.a. c. Royaume-Uni*, n° 58243/00, § 28.

1401 Cour eur. D.H., 12 janvier 2016, *Szabo et Vissy c. Hongrie*, n° 37138/14, § 68. La disposition visait « la prévention, le suivi et la répression des actes terroristes » ainsi que la collecte de « renseignements nécessaires à la sauvegarde de citoyens en détresse à l'étranger ». Celles-ci ont été considérées comme des indications suffisamment claires sur les circonstances et les conditions dans lesquelles les autorités publiques sont en droit d'avoir recours à une telle mesure. *Ibid.*, § 63.

1402 *Ibid.*, §§ 73 et 77.

307. L'autorisation de procéder à une mesure d'interception des communications par un service indépendant. Pour déterminer si la procédure d'autorisation est à même de garantir que la surveillance secrète n'est pas ordonnée au hasard, irrégulièrement ou sans examen approprié et convenable, la Cour eur. D.H. prend en compte un certain nombre de facteurs parmi lesquels, notamment, le service compétent pour autoriser la surveillance, la portée de l'examen qu'il effectue et le contenu de l'autorisation d'interception[1403]. Ce service ne doit pas forcément être un service « judiciaire », il doit néanmoins disposer d'une indépendance suffisante à l'égard de l'exécutif[1404].

308. La portée de l'examen à la lumière de l'examen d'un soupçon raisonnable ou individuel. La portée dudit examen revêt une importance particulière dans le cas où le champ d'application de la mesure d'interception de communications est large. Néanmoins, la latitude laissée aux autorités peut être contrebalancée par « une interprétation judiciaire établie de ces termes ou à une pratique consacrée consistant à vérifier au cas par cas s'il existe des raisons suffisantes d'intercepter les communications d'une personne donnée »[1405]. À titre illustratif, dans l'arrêt *Roman Zakharov*, la Cour considéra que cet examen doit permettre de vérifier la présence d'un « soupçon raisonnable » à l'égard de la personne concernée[1406], c'est-à-dire de « rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme par exemple des actes mettant en péril la sécurité nationale »[1407]. Dans l'arrêt *Szabo* par contre, la Cour admit la présence d'un « soupçon individuel » à l'encontre d'une personne pour justifier l'interception de ses communications[1408]. Cette décision fut vivement critiquée par le juge Pinto De Albuquerque[1409]. Selon ce dernier, en admettant la simple existence d'un « soupçon individuel », la Cour aurait élargi la possibilité de procéder à l'exécution d'un tel dispositif et aurait affaibli le critère retenu par la grande chambre dans l'arrêt *Roman Zakharov*[1410].

1403 Cour eur. D.H. (gr. ch.), 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06, § 257.
1404 *Ibid.*, § 258.
1405 *Ibid.*, § 249.
1406 *Ibid.*, § 260.
1407 *Ibid.*, § 260.
1408 Cour eur. D.H., 12 janvier 2016, *Szabo et Vissy c. Hongrie*, n° 37138/14, §§ 71 et 73.
1409 Opinion discordante du juge Pinto De Albuquerque, Cour eur. D.H., 12 janvier 2016, *Szabo et Vissy c. Hongrie*, n° 37138/14.
1410 Cour eur. D.H. (gr. ch.), 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06.