# Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information

De Terwangne, Cecile; Delforge, Antoine; Everarts de Velp, Sophie; Hocepied, Christian; Lognoul, Michael; Mont, Julie; Rosier, Karen; Tombal, Thomas

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

*Publication date:*
2021

*Document Version*
le PDF de l'éditeur

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

Cécile de Terwangne[312], Antoine Delforge[313], Sophie Everarts de Velp [314], Christian Hocepied[315], Michael Lognoul[316], Julie Mont[317], Karen Rosier[318], Thomas Tombal[319]

Sous la coordination de Antoine Delforge

**60. Introduction.** Cette chronique a pour but d'analyser les décisions de jurisprudence rendues entre 2018 et 2020 en matière de protection des données à caractère personnel, et plus généralement en matière de droit à la vie privée en lien avec les nouvelles technologies de l'information[320].

Cette période s'avère d'autant plus intéressante qu'en 2018, le Règlement général sur la protection des données (ci-après RGPD)[321] est entré en application. Certes, celui-ci ne révolutionne ni les principes fondamentaux ni les définitions clés, en matière de protection des données. Néanmoins, il a permis une mise à jour des règles de protection et une plus grande effectivité de celles-ci. Ainsi, dorénavant, l'Autorité de protection des données belge (ci-après l'APD), qui remplace l'ancienne Commission Vie Privée, a un véritable pouvoir de contrôle et sanction.

Nous nous limiterons ici à étudier les décisions rendues durant cette période par les juridictions belges, l'Autorité de protection des données belge (les décisions publiées sur son site internet[322]), ainsi que les juridictions européennes (Cour de justice et Cour européenne des droits de l'homme). Quelques décisions phares de la Commission Nationale de l'Informatique et des Libertés (CNIL – l'autorité de protection des données française) seront également évoquées.

Outre cette analyse des décisions rendues en application du RGPD (A), seront également abordées différentes décisions relatives à des législations plus spécifiques, telles que la législation en

312 Professeur à la Faculté de droit et directrice de recherche au Centre de recherche Information, Droit et Société (CRIDS) et Namur Digital Institute (NaDI), Université de Namur.

313 Assistant/chercheur au CRIDS/NaDI.

314 Chercheuse au CRIDS/NaDI, juriste.

315 Chercheur senior au CRIDS/NaDI.

316 Assistant/chercheur au CRIDS/NaDI.

317 Assistante/chercheuse au CRIDS/NaDI et avocate au Barreau de Namur.

318 Maître de conférences à l'Université de Namur, avocate au barreau du Brabant wallon et DPO.

319 Chercheur au CRIDS/NaDI.

320 Nous renvoyons aux précédentes chroniques publiées dans la *R.D.T.I.* concernant les décisions rendues avant 2018, voy. notamment C. Fievet, L. Gerard, N. Gillard, M. Knockart, A. Michel, J. Mont, K. Rosier, T. Tombal et O. Vanreck « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, H. Jacquemin et T. Tombal (coord.), *R.D.T.I.*, 2017, n° 68-69, pp. 94-163 ; C. Burnet, M. Piron, B. Losdyck, O. Vanreck, J.-M. Van Gyseghem, E. Degrave, C. Gayrel, J. Herveg et K. Rosier, « Libertés et société de l'information », *Chronique de jurisprudence en droit des technologies de l'information 2012*-2014, *R.D.T.I.*, 2015, n° 59-60, pp. 71 et s.

321 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.*, L 119, 14 mai 2016.

322 Quelques décisions publiées sur le site de l'APD n'ont pas été reprises dans cette chronique. En effet, certaines n'ont parfois qu'un intérêt très limité, notamment lorsqu'elles se limitent à un simple rappel de ce qui est écrit dans le RGPD. De plus, l'APD examinant dans ses décisions, quasi systématiquement, la qualification des acteurs concernés, la base de licéité des traitements, la violation des droits, et le non-respect de certaines mesures de *compliance*, il n'est pas possible d'évoquer l'ensemble de ces points pour chacune des décisions rendues.

matière de communication électronique[323] (B) et la loi « caméra »[324] (C). Enfin, la présente chronique intègre également une étude des principales décisions en matière d'usage de technologies de l'information et de la communication dans les relations de travail confronté au droit au respect de la vie privée (D), et en matière d'e-gouvernement (E)[325].

## A. Protection des données à caractère personnel

### *1. Champ d'application matériel*

**61. Traitement de données non automatisé – Notion de fichier.** Dans la période couverte par la présente chronique, la Cour de justice de l'Union européenne a été amenée à se prononcer sur la notion de fichier[326] contenue dans la directive 95/46[327]. Dans l'affaire en question, la Cour indique que la notion de fichier couvre notamment « un ensemble de données à caractère personnel collectées dans le cadre d'une activité de prédication de porte-à-porte, comportant des noms et des adresses ainsi que d'autres informations concernant les personnes démarchées, dès lors que ces données sont structurées selon des critères déterminés permettant, en pratique, de les retrouver aisément aux fins d'une utilisation ultérieure. Pour qu'un tel ensemble relève de cette notion, il n'est pas nécessaire qu'il comprenne des fiches, des listes spécifiques ou d'autres systèmes de recherche »[328]. En l'occurrence, l'interprétation donnée à la notion de fichier conditionnait l'applicabilité de la directive aux faits décrits par la juridiction de renvoi, s'agissant d'un traitement de données à caractère personnel non automatisé. Suivant l'interprétation faite par la C.J.U.E., les traitements en cause sont soumis aux dispositions de la directive 95/46.

**62. Activités religieuses – Exception à des fins purement personnelles ou domestiques.** Dans la même affaire[329], la C.J.U.E. était également interrogée sur l'applicabilité des exceptions au champ d'application de la directive 95/46, concernant les traitements de données pratiqués par la communauté religieuse en cause dans le cadre de son activité de prédication de porte-à-porte. Dans son arrêt, la Cour indique que les exceptions prévues par la directive ont trait aux activités purement étatiques, d'une part, et aux traitements de données effectués par des personnes physiques à des fins exclusivement personnelles ou domestiques, d'autre part[330]. Or, selon la Cour, les traitements en cause ne ressortent d'aucune de ces deux catégories[331], et doivent donc être soumis au champ d'application de la directive 95/46.

---

323 Nous nous limiterons ici aux décisions ayant un lien direct avec le droit à la vie privée (rétention de données, et usage de cookies). Pour les décisions en matière de communications électroniques relatives à d'autres aspects, nous renvoyons notamment au titre V « Communications électroniques » de la présente chronique.

324 Loi du 21 avril 2007 réglant l'installation et l'utilisation de caméras de surveillance.

325 Les décisions se rattachant plus spécifiquement aux communications électroniques dans le domaine de la recherche et poursuite des infractions sont analysées sous le titre VI « Criminalité informatique », §§ 319 et s.

326 C.J. (gde ch.), 10 juillet 2018, arrêt *Jehovan todistajat*, C-25/17.

327 Article 2, c), de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281/31, ci-après la directive 95/46. La notion étant identique au sein du RGPD (article 4, 6)), cet enseignement est toujours d'application.

328 C.J. (gde ch.), 10 juillet 2018, arrêt *Jehovan todistajat*, précité, point 62.

329 C.J. (gde ch.), 10 juillet 2018, arrêt *Jehovan todistajat*, précité.

330 Voy. art. 3, § 2, directive 95/46.

331 C.J. (gde ch.), 10 juillet 2018, arrêt *Jehovan todistajat*, précité, points 38-39 et 40-50.

**63. Vidéo montrant des membres de la police publiée sur YouTube – Applicabilité des exceptions.** Dans une affaire datant du 14 février 2019, la C.J.U.E. s'est prononcée sur l'applicabilité de la directive 95/46 dans une situation où une personne physique a filmé durant sa déposition une vidéo montrant des membres de la police dans leur commissariat[332]. Cette personne a ensuite publié la vidéo sur le site *YouTube*. Dans son arrêt, la Cour constate que les faits en cause constituent un traitement de données à caractère personnel au sens de la directive. En outre, la Cour relève que les exceptions au champ d'application de celle-ci ne trouvent pas à s'appliquer au cas d'espèce, à défaut d'activités purement étatiques ou de fins exclusivement personnelles ou domestiques liées au traitement des données litigieux. Elle en conclut que le champ d'application de la directive est rencontré, et indique que « le fait de procéder à un enregistrement vidéo de membres de la police dans le cadre de l'exercice de leurs fonctions n'est pas de nature à exclure un tel type de traitement de données à caractère personnel » de son champ d'application[333].

**64. Utilisateurs de réseaux sociaux – Exception à des fins exclusivement personnelles et responsabilité conjointe.** L'APD a récemment considéré que le fait pour les utilisateurs d'un réseau social d'envoyer, via une fonctionnalité « inviter un ami » proposée par ce réseau social, une invitation à rejoindre ledit réseau à ses proches relevait de l'exception à des fins strictement personnelles et domestiques pour les utilisateurs. Si ceux-ci ne doivent donc pas respecter le RGPD lors de l'utilisation de cette fonctionnalité, l'APD poursuit en rappelant le considérant 18 du RGPD[334], ce qui signifie que, dans le cas d'espèce, le réseau social qui lui aussi traite les données pour l'envoi de l'e-mail d'invitation est lui aussi responsable du traitement mais ne peut pas bénéficier de la même exception[335].

### *2. Questions de droit international public et privé*

#### *a. Compétence juridictionnelle*

**65. Cookies Facebook – Droit international public.** Dans son jugement au fond du 16 février 2018, relatif à la fameuse affaire des cookies de *Facebook*, le tribunal de première instance néerlandophone de Bruxelles établit sa compétence à l'égard de *Facebook inc.*, *Facebook Ireland Limited* et *Facebook Belgium*[336]. Pour ce faire, le tribunal a considéré que l'ancienne Commission de la protection de la vie privée (désormais Autorité de protection des données) exerçait l'autorité publique en attaquant en justice les pratiques litigieuses de *Facebook*[337]. Le tribunal en a déduit que le droit international public devait être utilisé pour déterminer la compétence juridictionnelle, en faisant application du principe de territorialité. Ainsi que le relève A. Michel, le tribunal

332 C.J., 14 février 2019, arrêt *Sergejs Buivids*, C-345/17. Voy. également l'analyse de cet arrêt dans la partie IV « Médias, liberté d'expression et nouvelles technologies », §§ 183 et s.

333 C.J., 14 février 2019, arrêt *Sergejs Buivids*, précité, point 44.

334 « […] Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ».

335 APD, 14 mai 2020, décision n° 25/2020. Sur la légalité du traitement, voy. *infra*, § 94.

336 Civ. Bruxelles, 16 février 2018, R.G. n° 2016/153/A, inédit. Pour un résumé des faits en cause et des procédures judiciaires antérieures, voy. la chronique précédente *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 96-97. Voy. également G. Dejemeppe, « L'affaire *Facebook* : questions de procédure », note sous Civ. Bruxelles (réf.) (ord.), 9 novembre 2015 et Bruxelles, 29 juin 2016, *R.D.T.I.*, 2016, n° 62, pp. 113 à 126.

337 Civ. Bruxelles, 16 février 2018, précité, point 40.

de première instance décide que « puisque les infractions reprochées au réseau social ont lieu et/ou sortent leurs effets en Belgique, que les personnes concernées et les appareils qu'elles utilisent sont présents sur le territoire belge et que la stratégie commerciale de Facebook vise également ce territoire, l'exigence de 'liens substantiels suffisants' avec la Belgique est remplie »[338].

Néanmoins, l'arrêt de la cour d'appel de Bruxelles du 8 mai 2019 infirme partiellement le jugement de première instance mentionné ci-devant, en matière de compétence juridictionnelle[339]. La cour d'appel confirme sa compétence vis-à-vis de *Facebook Belgium*[340], mais se déclare non compétente pour connaître des demandes contre *Facebook Ireland Limited* et *Facebook inc*. Elle considère, en l'espèce, que le principe de territorialité issu du droit international public n'est pas applicable pour déterminer la compétence des juridictions belges dans ce litige[341]. Au demeurant, la cour d'appel ne relève pas d'autre source de droit international public qui lui conférerait compétence *in casu*[342]. Pour le surplus, elle considère que le droit international privé ne lui permet pas non plus d'établir sa compétence vis-à-vis de *Facebook Ireland Limited* et *Facebook inc*[343].

*b. Champ d'application territorial*

**66. Moteur de recherche établi hors UE – Déréférencement.** Le 24 septembre 2019, la C.J.U.E. a rendu un arrêt traitant, notamment, du champ d'application territorial de la législation européenne relative à la protection des données à caractère personnel, suite à l'exercice du droit au déférencement envers le moteur de recherche *Google*[344]. Dans cette affaire, qui opposait la Commission nationale de l'informatique et des libertés française (CNIL) et *Google*, la Cour a considéré (conformément à sa jurisprudence antérieure[345]) que tant la directive 95/46 que le RGPD étaient applicables *ratione loci* aux traitements effectués par *Google*[346]. En effet, cette dernière traite des données à caractère personnel dans le cadre des activités de ses établissements sur le territoire des États membres, puisqu'elle y dispose d'établissements chargés d'assurer la promotion et la vente des espaces publicitaires proposés par *Google*, lesquels ciblent les habitants

338 A. Michel, « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des "cookies Facebook", véritable saga judiciaire ? », *R.D.T.I.*, 2019, n° 74, p. 78. Voy. également Civ. Bruxelles, 16 février 2018, précité, point 10.

339 Bruxelles, 8 mai 2019, *R.D.C.-T.B.H.*, 2020/1, pp. 75-91.

340 Bruxelles, 8 mai 2019, précité, p. 81. La Cour affirme sa compétence sur la base du seul droit belge, s'agissant d'une société de droit belge, attraite en justice devant une juridiction belge, par une autorité publique belge. Avant de se prononcer sur le fond de l'affaire, vis-à-vis de *Facebook Belgium*, la cour d'appel a toutefois posé plusieurs questions préjudicielles à la C.J.U.E., qui y a répondu en 2021 (voy. C.J. (gde ch.), 15 juin 2021, arrêt *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, C-645/19). Cette décision sera évoquée dans la prochaine chronique.

341 Bruxelles, 8 mai 2019, précité, p. 83.

342 *Idem.*

343 Bruxelles, 8 mai 2019, précité, pp. 85-87.

344 C.J. (gde ch.), 24 septembre 2019, arrêt *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17. Voy. également *infra*, § 105 de cette chronique sur la portée « territoriale » du droit au déréférencement.

345 La C.J.U.E. fait notamment référence à son arrêt *Google Spain* (C.J. (gde ch.), 13 mai 2014, arrêt *Google Spain SL et Google inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12). À ce sujet, nous renvoyons à l'une des chroniques précédentes, *Chronique de jurisprudence en droit des technologies de l'information 2012-2014*, *R.D.T.I.*, 2015, n° 59-60, pp. 77 et s.

346 En ce qui concerne la portée territoriale du droit au déréférencement dont il est question dans cette affaire, voy. l'analyse de cet arrêt faite, *infra* § 107, et dans la partie IV « Médias, liberté d'expression et nouvelles technologies » de cette chronique, §§ 225 et s.

desdits États membres[347]. Le fait que le moteur de recherche soit exploité par une entreprise d'un État tiers n'empêche donc pas, dans ces conditions, l'application du droit européen encadrant les traitements de données à caractère personnel.

**67. Responsable du traitement établi hors UE – Plainte classée sans suite.** Dans une décision du 15 juillet 2020, l'APD décide de classer la plainte d'un particulier sans suite, au motif notamment qu'il n'est pas certain que le RGPD s'applique *ratione loci* aux faits visés[348]. En l'occurrence, le plaignant avait déposé plainte auprès de l'APD après avoir constaté, via une plateforme en ligne nommée « Have I Been Pwned », qu'un traitement illicite de ses données par un responsable du traitement établi en Californie aurait eu lieu[349]. L'autorité belge ne donne toutefois pas plus d'informations quant aux éléments qui créent une telle incertitude dans son chef, pour déterminer si la législation européenne est applicable ou non aux faits en cause.

### *3. Définitions/notions*

**68. Étendue de la notion de données à caractère personnel[350].** Dans une décision du 30 octobre 2020, l'APD tranche un litige relatif à la publication, sur *YouTube*, d'une vidéo montrant un bien immeuble dont la cheminée évacue la fumée d'un feu de bois[351]. La personne publiant la vidéo y avait ajouté l'adresse dudit bien, et le nom de son occupant, afin de dénoncer ce qu'elle considère être une pollution de l'air. Du fait de cet ajout, l'APD décide que la qualification de données à caractère personnel doit être retenue pour l'ensemble de la publication sur le site internet, puisque les images de la cheminée et de la fumée (non identifiantes à l'origine) sont ainsi liées à d'autres données permettant l'identification de l'occupant de l'immeuble.

**69. Notion de données relatives aux infractions et aux condamnations pénales[352].** Dans l'arrêt précité du 24 septembre 2019[353], la C.J.U.E. considère que « les informations concernant une procédure judiciaire menée contre une personne physique, telles que celles relatant sa mise en examen ou le procès, et, le cas échéant, la condamnation qui en a résulté, constituent des données relatives aux "infractions" et aux "condamnations pénales" [au sens de la directive 95/46/CE et du RGPD], et ce indépendamment du fait que, au cours de cette procédure judiciaire, la commission de l'infraction pour laquelle la personne était poursuivie a effectivement été établie ou non »[354].

**70. Notion de catégories particulières de données à caractère personnel – Moteurs de recherche.** Dans cette même affaire du 24 septembre 2019, la C.J.U.E. a été appelée à se prononcer sur le champ d'application matériel des dispositions relatives aux catégories particulières de données à caractère personnel[355]. En l'espèce, plusieurs personnes physiques ont sollicité

347 C.J. (gde ch.), 24 septembre 2019, arrêt *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, précité, points 48-52.

348 APD, 15 juillet 2020, décision n° 38/2020.

349 *Idem*, point 2.

350 Article 4, 1), RGPD.

351 APD, 30 octobre 2020, décision n° 71/2020.

352 Article 10, RGPD.

353 C.J. (gde ch.), 24 septembre 2019, arrêt *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés (CNIL)*, précité.

354 *Idem*, point 72.

355 C.J. (gde ch.), 24 septembre 2019, arrêt *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés (CNIL)*, précité. Voy. également l'analyse de cet arrêt faite *infra*, § 105, ainsi que dans la partie IV « Médias, liberté d'expression et nouvelles technologies », §§ 230 et s.

le déréférencement de liens auprès de *Google*, chacun des liens ayant trait à des catégories spécifiques de données à caractère personnel (notamment, des données concernant la vie sexuelle et des données judiciaires). *Google* ayant refusé de donner suite à ces requêtes, il est demandé à la Cour de déterminer si (et comment, le cas échéant) les règles relatives au traitement des catégories particulières de données à caractère personnel s'appliquent aux moteurs de recherche[356].

Considérant que l'activité d'un moteur de recherche consiste notamment en des traitements (de catégories particulières) de données à caractère personnel, joue un rôle décisif dans la diffusion de telles données, et ne bénéficie d'aucune dérogation prévue par les dispositions applicables, la Cour constate que cette activité doit en principe satisfaire aux règles relatives au traitement de ces types de données. Néanmoins, la Cour prend en compte le rôle particulier que jouent les moteurs de recherche en ligne, et note que « l'exploitant d'un moteur de recherche est responsable non pas du fait que des données à caractère personnel visées par lesdites dispositions figurent sur une page web publiée par un tiers, mais [est responsable] du référencement de cette page ». De ce fait, les dispositions relatives au traitement de catégories particulières de données à caractère personnel ne s'appliquent aux moteurs de recherche « qu'en raison de ce référencement, et, donc, par l'intermédiaire d'une vérification à effectuer, sous le contrôle des autorités nationales compétentes, sur la base d'une demande formée par la personne concernée »[357].

**71. Notion de traitement**[358]**.** La décision rendue par l'APD le 30 juin 2020 qualifie l'envoi par mail de la photo de profil mise en ligne sur *Facebook* d'une personne physique à des tiers, d'opération de traitement[359]. Sur le plan factuel, il s'agissait pour le responsable de ce traitement de communiquer à des commissaires sportifs une interdiction de fréquentation prononcée par le tribunal du sport, accompagnée par la photo de l'individu concerné par l'interdiction. L'APD considère, *in casu*, que le fait que la photo n'était pas structurée selon des critères déterminés n'est pas pertinent pour écarter la qualification de traitement, dès lors que ledit traitement n'est pas manuel, mais bien effectué avec des moyens automatisés.

**72. Notion de responsable du traitement**[360]**.** L'arrêt rendu par la C.J.U.E. le 5 juin 2018[361] clarifie la notion de responsable du traitement, de telle sorte que ladite notion peut englober désormais l'administrateur d'une *fanpage*, hébergée sur le réseau social *Facebook*. Pour parvenir à cette conclusion, la C.J.U.E. considère que « l'administrateur d'une page fan hébergée sur Facebook, tel que Wirtschaftsakademie, participe, par son action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan. De ce fait, cet administrateur doit être, en l'occurrence, qualifié de responsable au sein

356 Voy. art. 8, § 1 et 5, directive 95/46, et art. 9, § 1, et 10, RGPD.
357 C.J. (gde ch.), 24 septembre 2019, arrêt *GC, AF, BH, ED c. CNIL*, précité, point 47.
358 Article 4, 2), RGPD.
359 APD, 30 juin 2020, décision n° 35/2020.
360 Article 4, 7), RGPD.
361 C.J. (gde ch.), 5 juin 2018, arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16.

de l'Union, conjointement avec Facebook Ireland, de ce traitement »[362]. En répondant de la sorte, la Cour semble d'ailleurs multiplier les cas de responsabilité conjointe possibles[363].

La juridiction européenne a également apporté quelques précisions sur la notion de responsable du traitement, dans son arrêt précité du 10 juillet 2018[364]. En l'espèce, elle décida qu'une communauté religieuse pouvait être considérée « comme étant responsable, conjointement avec ses membres prédicateurs, des traitements de données à caractère personnel effectués par ces derniers dans le cadre d'une activité de prédication de porte-à-porte organisée, coordonnée et encouragée par cette communauté, sans qu'il soit nécessaire que ladite communauté ait accès aux données ni qu'il doive être établi qu'elle a donné à ses membres des lignes directrices écrites ou des consignes relativement à ces traitements »[365].

Dans un troisième arrêt, qui traite de la notion de responsable du traitement[366], la Cour considéra que le gestionnaire d'un site internet, qui intègre sur ce dernier un module social (en l'occurrence, le bouton « j'aime » de *Facebook*) qui transmet automatiquement des données à caractère personnel au fournisseur du module, pouvait être qualifié de responsable du traitement pour les traitements auxquels il participe effectivement, c'est-à-dire « la collecte et la communication par transmission des données en cause »[367].

Au niveau belge, l'APD a, en outre, rendu quelques décisions intéressantes concernant la notion de responsable du traitement. Dans la première décision, rendue le 30 juin 2020 (précitée)[368], l'APD considère que la qualification de responsable du traitement ne revient pas à l'employé ayant transmis la photo de profil *Facebook* d'une personne physique par e-mail, au nom et pour compte de son employeur. Ladite qualification revient, logiquement, à l'employeur.

Dans la seconde décision, rendue le 30 juillet 2020[369], l'APD doit déterminer si *Proximus S.A.* répond à la notion de responsable du traitement, vis-à-vis de traitements de données à caractère personnel d'une personne physique, dans le cadre de son activité d'élaboration d'annuaires et d'offre de services de renseignements téléphoniques. Pour ce faire, l'APD commence par lister les divers traitements en présence[370]. Elle analyse ensuite, *in concreto*, si *Proximus S.A.* (i) détermine[371] (ii) les finalités et les moyens des traitements en cause. Elle en conclut que *Proximus S.A.* est responsable d'une partie des traitements en cause, d'autres responsables du traitement étant désignés par l'APD pour l'autre partie des traitements en cause.

Enfin, l'APD a considéré que, concernant l'envoi d'e-mail d'invitation à rejoindre un réseau social par les utilisateurs de ce réseau social, tant l'utilisateur lui-même que ledit réseau social devaient

362 C.J. (gde ch.), 5 juin 2018, arrêt *Wirtschaftsakademie*, précité, point 39. Nous renvoyons également à la *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 108 et s.

363 Pour une étude plus détaillée des conséquences pratiques de cet arrêt, nous renvoyons à S. Xefteri, « La responsabilité conjointe de l'exploitant du réseau social et de l'administrateur d'une page fan », *Rev. aff. eur.*, 2018/2, pp. 39-401.

364 C.J. (gde ch.), 10 juillet 2018, arrêt *Jehovan todistajat*, précité.

365 *Idem*, point 75.

366 C.J., 29 juillet 2019, arrêt *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, C-40/17.

367 *Idem*, point 85.

368 APD, 30 juin 2020, décision n° 35/2020.

369 APD, 30 juillet 2020, décision n° 42/2020.

370 APD, 30 juillet 2020, décision n° 42/2020, point 45.

371 L'APD entend par là « prendre l'initiative des traitements en cause », voy. APD, 30 juillet 2020, précité.

être considérés comme responsables de ce traitement, même si le premier pouvait bénéficier de l'exception prévue à l'article 2 du RGPD (« exception domestique »)[372].

### *4. Principes généraux*

**73. Introduction.** À son article 5, le RGPD fait référence à plusieurs grands principes généraux. À la lecture des différentes décisions analysées, il nous parait pertinent de commenter en particulier trois de ces principes, à savoir celui de transparence, de finalité, ainsi que de minimisation de données (et de limitation de la durée du traitement).

#### *a. Principe de transparence*

**74. Réponse aux demandes des personnes concernées[373].** La transparence en matière de protection des données doit être respectée à toutes les étapes du traitement (avant et après la collecte des données)[374]. Ainsi, l'APD a rappelé qu'il convient d'être transparent dans sa réponse en cas de questionnement par la personne concernée. Dans une décision du 17 septembre 2019, l'APD a estimé que « plutôt que de déclarer [à l'APD] ne pas avoir pu procéder à la suppression des données à caractère personnel du plaignant, en raison du fait que les données de la personne concernée n'auraient pas été enregistrées dans son fichier de données, le défendeur aurait dû également informer le plaignant de cet élément, ce qui n'a toutefois pas été fait »[375].

Dans une autre décision, l'APD relève le manque de transparence dans la réponse de *Google Belgique* à une demande de déréférencement. En effet, la personne concernée s'est trouvée confrontée à un motif de refus de sa demande ne lui permettant ni de connaître ni de comprendre complètement la motivation de *Google Belgique*. L'APD a jugé que l'entreprise avait manqué de transparence et n'avait pas été suffisamment compréhensible dans sa réponse[376].

**75. Langue de la politique de confidentialité.** L'APD a rappelé que la langue utilisée pour informer les personnes concernées dans sa « privacy policy » devait correspondre à celle du public cible du site web, et donc pas l'anglais pour un public belge[377]. À cette occasion, elle a également rappelé que les politiques de cookies et de confidentialité doivent en outre être facilement accessibles, sans que cela ne nécessite une démarche compliquée pour la personne concernée.

**76. Précision et clarté de la politique de confidentialité.** S'il est vrai que la rédaction d'une politique de confidentialité peut s'avérer technique et que parfois, celle-ci peut vite devenir complexe à lire, le responsable doit néanmoins s'assurer que celle-ci reste précise et claire. Dans le cadre d'une affaire concernant la conformité d'une politique de confidentialité d'un site web[378], le gestionnaire du site n'avait pas établi de distinction claire entre le traitement de données de santé et le traitement des autres données à caractère personnel dites ordinaires. Une telle distinc-

372 APD, 14 mai 2020, décision n° 25/2020. Voy. *supra*, § 64 pour plus de détails.

373 Voy. également *infra*, §§ 99 et s. Il est en effet fréquent que l'APD considère que la violation du principe général de transparence soit liée à la violation des prescrits encadrant le droit à l'information et le droit d'accès de la personne concernée.

374 Voy. art. 5, 12, 13 et 14 du RGPD.

375 APD, 17 septembre 2019, décision n° 8/2019.

376 APD, 14 juillet 2020, décision n° 37/2020.

377 APD, 17 décembre 2019, décision n° 12/2019. Voy. également *infra*, §§ 87 et s.

378 APD, 14 mai 2020, décision n° 4/2020.

tion est néanmoins d'une importance fondamentale pour déterminer le fondement juridique sur lequel le traitement peut se baser pour une finalité déterminée ou un transfert à un tiers. L'absence de distinction crée la confusion en affirmant ne pas traiter de données de santé pour la finalité « de prévention des abus et de la fraude », alors que le formulaire de consentement mentionne l'inverse en demandant le consentement de la personne concernée à ces mêmes fins.

La personne concernée devrait donc être en mesure de déterminer à l'avance la portée et les conséquences du traitement afin de ne pas être prise au dépourvu quant à la façon dont ses données à caractère personnel ont été utilisées. À ce titre, l'APD estime « que les informations mentionnées doivent être concrètes et fiables, qu'elles ne doivent pas être formulées dans des termes abstraits ou ambigus ni laisser de place à différentes interprétations », ce qui est notamment le cas lorsque des termes tels que « autres finalités » (précision insuffisante) ou des concepts jamais clairement définis sont utilisés[379]. De plus, elle tient à indiquer que l'absence de demande d'éclaircissement concernant ces formulations vagues ne peut être considérée comme un argument valable pour juger ces formulations comme étant suffisamment précises, et respectant le RGPD.

Par sa décision n° 73/2020[380], l'APD fait également état d'un manque de transparence dans la politique de confidentialité d'une société de logements, suite à la confusion créée par l'utilisation de différents termes pour parler de la même chose (« informations », « données », « données à caractère personnel ») et le caractère « incompréhensible » et non adaptés de ceux-ci par rapport au profil des personnes concernées (« locataires à bas revenus […] disposant d'un niveau d'études peu élevé »).

La décision du 21 janvier 2019 de la Commission Nationale de l'Informatique et des Libertés (CNIL – l'autorité de protection des données française) mérite également d'être évoquée. La CNIL a en effet imposé une amende de cinquante millions d'euros à *Google* pour un manque de transparence et d'accessibilité des informations relatives aux traitements de données à caractère personnel que cette société effectue, ainsi que pour une absence de base de licéité de traitement appropriée[381]. Sur le premier aspect[382], la CNIL a estimé que la politique de confidentialité et les conditions d'utilisation de *Google* ne répondaient pas à l'exigence de transparence de l'article 12 du RGPD, en raison d'un manque général d'accessibilité des informations relatives aux traitements de données à caractère personnel que cette société effectue, dû à l'architecture « multicouche » (multiples renvois de page en page) utilisée par *Google*, qui a pour effet que les informations en cause sont excessivement dispersées dans de multiples documents[383]. De plus, la CNIL a estimé que l'information n'était pas claire et intelligible, car elle ne permettait pas aux personnes concernées de suffisamment comprendre les différentes finalités du traitement, qui étaient trop génériques, imprécises et incomplètes[384]. Ceci a été considéré comme particulièrement problématique par la CNIL compte tenu de la très grande quantité de données traitées, y

379 APD, 29 juillet 2020, décision n° 41/2020.
380 APD, 13 novembre 2020, décision n° 73/2020.
381 CNIL, *Google*, 21 janvier 2019, délibération SAN-2019-001.
382 Sur la question de la licéité du consentement, voy. *infra*, §§ 87 et 88.
383 CNIL, *Google*, 21 janvier 2019, précité, §§ 96-103.
384 *Ibid.*, §§ 104-128.

compris certaines catégories de données sensibles[385]. Cette décision de la CNIL a été confirmée par le Conseil d'État français[386].

**77. Politique de confidentialité pour des cookies.** Dans son désormais célèbre arrêt *Planet49*[387], la C.J.U.E. a clarifié quelles informations devaient être communiquées lors du placement de cookies sur l'appareil d'un utilisateur. Le responsable du traitement doit notamment fournir des informations sur la durée de fonctionnement des cookies ainsi que sur la possibilité ou non pour des tiers d'avoir accès à ces cookies, afin de garantir des informations équitables et transparentes.

Plus récemment, par deux décisions du 7 décembre 2020, la CNIL a imposé à *Google* une amende de cent millions d'euros, et à *Amazon* une amende de trente-cinq millions d'euros, pour avoir placé des *cookies* publicitaires sur les ordinateurs des utilisateurs de www.google.fr / www.amazon.fr, résidant en France, sans consentement préalable[388] et sans information suffisante[389]. Sur ce second aspect, la CNIL a jugé dans l'affaire *Google* que les informations fournies par cette société, tant dans le bandeau apparaissant en bas de la page internet que dans la fenêtre surgissante (*pop-up*), ne permettaient pas aux utilisateurs, lors de leur arrivée sur www.google.fr, d'être clairement et préalablement informés de l'existence de traitements permettant le dépôt de *cookies* sur leur terminal et l'accès aux informations contenues dans ces *cookies*[390]. Par conséquent, les informations fournies par *Google* ne permettaient pas aux utilisateurs d'être clairement et préalablement informés des finalités de ces traitements et des moyens pouvant être mis en œuvre pour s'y opposer[391]. Pareillement, concernant *Amazon*, la CNIL a jugé que les informations relatives aux *cookies* fournies par *Amazon* à ses utilisateurs étaient soit inexistantes, soit incomplètes[392]. En effet, la CNIL a jugé que la bannière d'information figurant sur la page d'accueil du site www.amazon.fr ne contenait qu'une description générale et approximative de la finalité des *cookies*, et qu'elle ne fournissait aucune information sur les moyens mis à la disposition des utilisateurs pour s'opposer à leur utilisation[393]. Pour la CNIL, la violation du principe de transparence était encore plus flagrante pour les utilisateurs arrivant sur le site www.amazon.fr par le biais d'une publicité publiée sur le site web d'un tiers, car, dans ce cas, absolument aucune information n'était fournie aux utilisateurs concernant ces *cookies*.

**78. Transparence – Missions d'un détective privé.** Même un détective privé a l'obligation d'être transparent quant à ses activités et doit avertir la personne concernée de l'existence du traitement de ses données et de ses finalités, préalablement à la mise en œuvre du traitement.

385 CNIL, *Google*, 21 janvier 2019, précité, § 109.

386 Conseil d'État, *Société Google LLC*, 19 juin 2020, décision n° 430810.

387 C.J. (gde ch.), 1er octobre 2019, arrêt *Planet49*, précité. Dans le même sens, APD, 17 décembre 2019, décision n° 12/2019. Pour un commentaire plus développé sur ces arrêts, voy. *infra*, §§ 124 et s.

388 Sur cette question du consentement, voy. *infra*, § 126.

389 CNIL, *Google LLC and Google Ireland Limited*, 7 décembre 2020, délibération SAN-2020-012 ; CNIL, *Amazon Europe Core*, 7 décembre 2020, délibération SAN-2020-013.

390 CNIL, *Google LLC and Google Ireland Limited*, 7 décembre 2020, précité, § 82.

391 *Ibidem*. À cet égard, il convient de souligner que même si Google a pris des mesures, au cours de la procédure, pour fournir au préalable davantage d'informations, la CNIL a considéré que ces informations étaient encore trop imprécises, car elles ne permettaient toujours pas aux utilisateurs de comprendre les finalités du traitement ni les moyens mis à leur disposition pour s'opposer à leur utilisation (voy. les §§ 86 à 94 de cette décision).

392 CNIL, *Amazon Europe Core*, 7 décembre 2020, précité, § 92.

393 *Ibid.*, §§ 94-95.

Ainsi, dans un arrêt du 4 février 2018, la cour d'appel de Mons tranche sur la recevabilité en justice du rapport rédigé par un détective privé, dans une affaire entre un assureur et son assuré[394]. Le détective privé, mandaté par l'assureur pour établir la véracité et le montant du dommage subi par l'assuré, a informé ce dernier de son identité, de sa qualité de détective, et de l'identité de son mandataire. Il a également informé l'assuré de l'objet de sa collecte de données, c'est-à-dire la gestion du sinistre litigieux. En revanche, il n'a pas communiqué à l'assuré des informations relatives au caractère obligatoire ou non de ses réponses ni quant aux conséquences d'un éventuel défaut de réponse. Selon la Cour, ces éléments satisfont toutefois à l'obligation d'information prévue par la réglementation en vigueur à l'époque[395], de telle sorte que l'omission du détective n'est pas déterminante, et que le rapport du détective est recevable comme preuve[396].

Toujours en ce qui concerne des détectives privés, la Cour de cassation belge a considéré, dans un arrêt traitant de la recevabilité en justice d'un rapport d'un détective privé[397], qu'il est satisfait à l'obligation spécifique[398] d'information de la personne concernée, dès lors que le rapport du détective privé avait été communiqué à la personne concernée avant la procédure judiciaire opposant les parties[399].

*b. Principe de finalité*

**79. Introduction.** Les données à caractère personnel doivent être collectées dans un but bien déterminé et légitime et ne peuvent, en aucun cas, être *traitées ultérieurement de façon incompatible* avec cet objectif initial. Ces finalités doivent être *explicitement* indiquées à la personne concernée. Plusieurs affaires analysées précisent ces éléments.

**80. Finalité explicite.** Dans le cadre d'un recours au sujet d'un traitement de données à des fins de prélèvement direct sur le salaire des affiliés à un syndicat de leur cotisation syndicale, l'APD estime que ce n'est qu'après sa propre analyse approfondie du traitement litigieux que la finalité du traitement a pu être éclaircie. Elle en conclut, dès lors, assez logiquement, qu'une finalité nécessitant ce type d'examen pour être clarifiée ne peut être considérée comme étant suffisamment explicite[400].

**81. Traitement ultérieur compatible.** Dans deux affaires concernant la réutilisation à des fins électorales de données collectées dans le cadre des fonctions de bourgmestre, l'APD eut l'occasion de réaffirmer ce principe de finalité déterminée et l'impossibilité de réutiliser des données pour des finalités ultérieures non compatibles avec la finalité initiale du traitement[401].

394 Mons, 4 février 2018, *R.G.A.R.*, 2019/2, 15551.

395 Article 9 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, abrogée depuis par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

396 Mons, 4 février 2018, précité, point 3.4.

397 Cass., 14 septembre 2020, R.G. n° S.18.0099.F.

398 Article 9 de l'ancienne loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

399 Cass., 14 septembre 2020, précité.

400 APD, 9 novembre 2020, décision n° 72/2020.

401 APD, 25 novembre 2019, décisions n° 10/2019 et n° 11/2019. Pour plus de précisions sur ces deux décisions, voy. *infra*, § 162. D'autres décisions du même genre y sont également mentionnées.

Par ailleurs, a été classée sans suite une plainte au sujet d'une divulgation d'un rapport médical dans le cadre d'une procédure judiciaire. En effet, aucune violation des articles 6.1 et 9 du RGPD ne peut être constatée dans le chef du médecin désigné comme expert médical par le tribunal, vu qu'en application de l'article 973, § 1er, du Code judiciaire, le médecin avait l'obligation légale de mettre l'intégralité du rapport psychiatrique transmis au tribunal à la disposition de toutes les parties au procès. Vu que ce « nouveau » traitement repose sur une autre base de licéité, ceci peut être considéré comme une finalité séparée et non un détournement de finalité[402].

Dans une décision datant du 30 juin 2020[403], l'APD a également précisé que tant la consultation que l'utilisation d'une photo postée sur *Facebook* constituent un traitement au sens du RGPD, traitement qui doit se baser sur des finalités précises. Le fait que la photo en question ait été rendue accessible librement par la personne concernée elle-même (sur *Facebook*) n'autorise nullement la libre réutilisation de la photo par des tiers qui la consultent.

*c. Minimisation des données*

**82. Respect du principe de minimisation par le secteur public.** Le non-respect du principe de minimisation des données est régulièrement un des points soulevés par l'APD dans les décisions qu'elle rend. En effet, il est fréquent qu'à l'occasion d'une analyse des traitements opérés, elle constate de manière incidente que ce principe n'est pas respecté.

Cela a notamment été le cas concernant des affaires où certains organismes ont accédé, sans que cela soit justifié, à différentes bases de données publiques. Ainsi, l'APD a précisé que l'accès aux données contenues dans la DIV (service des immatriculations des véhicules belges) opéré par une société de gestion des stationnements dès le lendemain du contrôle du véhicule de la plaignante, est uniquement nécessaire pour l'envoi d'un rappel envoyé à son nom et à son adresse, et non avant[404].

A également été considéré comme ne respectant pas ce principe de minimisation le fait pour le SPF Finances de permettre aux citoyens de se connecter de manière plus conviviale au site FisconetPlus via un compte Microsoft (à créer ou préexistant), ce qui entraînait le traitement de données supplémentaires (par un tiers comme *Microsoft* de surcroît), alors même qu'il était également proposé une méthode de connexion à ce site sans passer par *Microsoft*, ceci prouvant même le caractère non nécessaire de la connexion à un compte Microsoft[405].

Le 9 juin 2020, la justice de paix de Forest a donné raison à un utilisateur de la STIB qui ne validait pas son abonnement à la borne électronique à chaque fois qu'il se déplaçait dans les transports en commun bruxellois. L'utilisateur disposait pourtant d'un abonnement annuel de transport auprès de la STIB qu'il avait payé régulièrement. Lors d'un contrôle, le plaignant s'est vu infliger une amende pour non-validation de sa carte MOBIB lors de son entrée dans le bus. L'utilisateur

402 APD, 27 août 2020, décision n° 51/2020.

403 APD, 30 juin 2020, décision n° 35/2020.

404 APD, 23 décembre 2020, décision n° 81/2020. Pour plus de détails sur cette décision, voy. *infra*, § 168.

405 APD, 23 décembre 2020, décision n° 82/2020. Dans cette même affaire, l'APD a également considéré que l'utilisation d'un compte *Microsoft* pour se connecter entraînait également une violation de l'article 6, premier alinéa et 7, du RGPD puisqu'il nécessitait l'installation de cookies non essentiels, sans l'obtention de consentement valable au préalable.

refusa de payer ces frais, estimant que la validation systématique de la carte MOBIB aux bornes électroniques constituait une atteinte à sa vie privée. Le juge de paix a estimé que le traitement des données de validation tel qu'il est actuellement effectué par la STIB n'était pas légal au motif qu'« il n'est pas clair dans quel cas le croisement des données "clients" et "validations" est nécessaire pour la répression des fraudes ». La justice de paix considère en effet que la mise en place d'un système complexe et de croisement de données entrainant « le suivi de l'historique des déplacements des usagers, [est] très intrusi[ve] du point de vue de la vie privée », en l'absence de justification suffisante venant de la STIB[406].

**83. Utilisation de la carte d'identité pour créer une carte de fidélité**. Sur la base de ce même principe de minimisation des données, l'APD a condamné à 10.000 EUR un commerce qui imposait la lecture de la carte d'identité électronique et l'utilisation des données de celle-ci pour la création d'une carte de fidélité[407].

**84. Expertise judiciaire et minimisation**. En matière d'expertise médicale, l'APD a estimé que des directives devaient être promulguées en ce qui concerne l'application du principe de minimisation des données dans le cadre du traitement de données sensibles par des experts lors de l'établissement de rapports d'expertise judiciaire. Pour l'instant, la violation du principe de minimisation ne peut pas être reprochée à un expert médical, vu que ce dernier a dans certains cas l'obligation légale de communiquer les données à caractère personnel aux juridictions judiciaires[408].

**85. Limitation de la durée de conservation – Conservation des données à des fins de défense en justice.** Le Conseil national des médecins a fait état d'une situation problématique concernant la durée de conservation des données lorsqu'un médecin est salarié d'un organisme public ou privé. En effet, ce dernier doit consigner ses constatations médicales dans un dossier organisé et conservé par son employeur, qui en est le responsable du traitement. Par ailleurs, lorsqu'un médecin est indépendant, une fois sa mission achevée, il retourne le dossier médical qu'il a constitué à celui qui l'a chargé de la mission, lequel est responsable de sa conservation. Le médecin chargé d'une mission n'a donc pas non plus à conserver les données une fois la mission terminée. Cependant, le Conseil national des médecins déclare qu'il peut se justifier que le médecin conserve dans ses archives la lettre de mission et le rapport du déroulé de celle-ci, et ce afin de pouvoir se défendre en cas de contestation[409].

### *5. Licéité du traitement*

**86. Introduction.** La condition de licéité du traitement, qui implique que le responsable du traitement doit pouvoir fonder son traitement sur une des hypothèses définies limitativement par le RGPD, a fait l'objet de plusieurs décisions durant la période étudiée, en particulier en ce

406 Justice de paix de Forest, 9 juin 2020, *T. Vred. / J.J.P.*, 2020/11-12, pp. 686-693. L'absence de base de licéité valide était aussi un des points soulevés.

407 APD, 17 septembre 2019, décision n° 6/2019. Cette décision a été depuis annulée par la Cour des marchés (pour des motifs touchant plutôt à la justification de la décision de l'APD, et non sur la validité de cette pratique). Pour plus de détails sur ce cas, voy. *infra*, § 163.

408 APD, 27 août 2020, décision n° 51/2020.

409 Conseil national de l'ordre des médecins, 5 juillet 2019, *R.G.A.R.*, 2019/9, pp. 15615-15616.

qui concerne le recours à un consentement de la personne concernée (art. 6.1.a) du RGPD) et à l'intérêt légitime du responsable (art. 6.1.f) du RGPD).

*a. Consentement de la personne concernée*

**87. Caractère éclairé.** Dans sa décision du 9 novembre 2020[410], l'APD rappelle l'obligation d'obtenir un consentement *éclairé* et donc logiquement la nécessité que la personne concernée ait notamment reçu les informations suivantes : l'identité du responsable de traitement ; la finalité de chacune des opérations de traitement pour lequel le consentement est sollicité ; les données qui seront collectées et utilisées ; l'existence d'un droit de retirer son consentement. En l'occurrence, les travailleurs n'avaient pas reçu d'informations sur leur droit de retirer leur consentement. Le consentement a dès lors été déclaré par l'APD comme étant non éclairé.

La décision précitée[411] du 21 janvier 2019 de la CNIL, imposant une amende de cinquante millions d'euros à *Google*, mérite également d'être évoquée[412]. En effet, la CNIL a jugé que le consentement que *Google* avait recueilli auprès de ses utilisateurs, au titre de base de licéité de traitement, n'était pas suffisamment « éclairé », et n'était donc pas valable, compte tenu du manque de transparence et d'accessibilité des informations relatives aux traitements de données à caractère personnel que cette société effectue[413].

**88. Caractère univoque.** La C.J.U.E., dans son arrêt *Orange Romania*[414], rappelle que le consentement d'une personne doit se manifester d'une manière libre, spécifique et informée et *univoque*. Tel n'est pas le cas lorsque sont utilisées des cases cochées par défaut ou tout autre mécanisme basé sur la passivité du client lors de la signature de contrats relatifs à la fourniture de services de télécommunications. Ainsi, l'APD a estimé, dans sa décision du 17 décembre 2019[415], que le site internet analysé contenait des cases précochées pour les préférences en matière de cookies, ce qui ne vaut pas consentement selon le considérant 32 du RGPD. À cet égard, il convient de se référer à l'arrêt *Planet 49*[416], dans lequel la C.J.U.E. répète ces mêmes règles.

Dans la décision de la CNIL mentionnée au point précédent, l'autorité française a également estimé que les consentements des personnes concernées n'étaient pas « univoques » et dénués d'ambiguïté, car ils n'ont pas été donnés par un acte positif clair, dès lors que la possibilité de donner un consentement spécifique pour chaque finalité n'était pas offerte avant les options « Tout Accepter » ou « Tout Refuser », et qu'elle était subordonnée à la nécessité pour les personnes concernées d'effectuer une action particulière, telle que cliquer sur « Plus d'options »[417].

**89. Consentement pré-RGPD.** À l'occasion d'une décision du 17 septembre 2019[418], l'APD a validé le fait d'envoyer un mail aux personnes qui se trouvaient déjà dans une base de données

410 APD, 9 novembre 2020, décision n° 72/2020.
411 Voy. *supra*, § 76.
412 CNIL, *Google*, 21 janvier 2019, délibération SAN-2019-001.
413 *Ibid.*, §§ 141-148.
414 C.J., 11 novembre 2020, arrêt *Orange Romania*, C-61/19.
415 APD, 17 décembre 2019, décision n° 12/2019 ; pour plus d'informations, voy. *infra*, §§ 124 et s.
416 C.J. (gde ch), 1er octobre 2019, arrêt *Planet49*, C-673/17. Pour un commentaire plus développé, voy. *infra*, §§ 124 et s.
417 CNIL, *Google*, 21 janvier 2019, précité, §§ 149-167.
418 APD, 17 septembre 2019, décision n° 8/2019. La Chambre contentieuse a également sanctionné le défendeur, car son registre des activités de traitement ne répondait pas à toutes les exigences du RGPD.

avant l'entrée en vigueur du RGPD en les invitant à donner explicitement leur consentement pour continuer à être reprises dans ladite base de données. Elle se garde toutefois de se prononcer « sur la façon dont la collecte de données s'était déroulée à l'époque ».

**90. Consentement des enfants**[419]**.** L'APD a été amenée à se prononcer sur la légalité d'une « enquête bien-être » auprès d'enfants d'une école, au moyen du système *SmartSchool*. L'un des points litigieux concernait la base de licéité du traitement, c'est-à-dire la validité du consentement donné par les enfants. *SmartSchool* étant un service d'enquête de satisfaction accessible via un navigateur web, donc un service de la société de l'information selon l'APD, cette dernière a considéré que l'article 8 du RGPD devait s'appliquer et qu'il aurait été donc nécessaire d'obtenir le consentement des personnes exerçant l'autorité parentale sur chaque élève de moins de 13 ans ayant participé à cette enquête[420].

**91. Retrait du consentement – Annuaire téléphonique.** Dans sa décision du 30 juillet 2020, l'APD a été confrontée à une affaire concernant une demande d'un abonné à un opérateur téléphonique de ne plus apparaitre dans deux annuaires électroniques gérés par le défendeur. Cette affaire est particulière du fait qu'au moment d'analyser la base de licéité, il faut, non seulement se référer aux articles 6.1.a) et 7 du RGPD, mais aussi à l'article 133 de la LCE. En effet, cet article prévoit qu'il est nécessaire d'obtenir le consentement de l'abonné pour apparaitre dans ce type d'annuaire. Toutefois, la législation belge ne précise pas de condition spécifique pour le retrait de ce consentement. L'APD en déduit qu'il faut dès lors se référer exclusivement au RGPD. La personne bénéficie donc bien d'un droit à demander à être retiré de ces annuaires, et le responsable de ces annuaires doit faire suivre cette demande de ne plus apparaitre dans des annuaires aux tiers avec lesquels il a partagé ces coordonnées[421].

*b. Intérêt légitime du responsable du traitement*

**92. Test de pondérations des intérêts respectifs.** Afin de pouvoir invoquer comme fondement de licéité son intérêt légitime, conformément à l'article 6.1.f) du RGPD, le responsable du traitement doit démontrer que :

- les intérêts qu'il poursuit avec le traitement peuvent être reconnus comme légitimes (le « test de finalité ») ;
- le traitement envisagé est nécessaire pour réaliser ces intérêts (le « test de nécessité ») ; et
- la pondération de ces intérêts par rapport aux intérêts, libertés et droits fondamentaux des personnes concernées pèse en faveur du responsable du traitement (le « test de pondération »). Il faut plus spécialement évaluer si « la personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée ».

419 Art. 8 du RGPD.

420 L'APD précisa à cette occasion que l'article 8 du RGPD ne prévoyait pas de communication spécifique à destination des parents, malgré le fait que c'est à eux de donner leur consentement. Seuls les enfants devaient être valablement informés, en utilisant des moyens de communication et un vocabulaire adapté à leur âge. Voy. APD, 16 juin 2020, décision n° 31/2020.

421 APD, 30 juillet 2020, décision n° 42/2020.

Ce dernier test est développé par la C.J.U.E. dans son arrêt *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*[422], qui précise que « sont également pertinentes aux fins de cette pondération les attentes raisonnables de la personne concernée à ce que ses données à caractère personnel ne seront pas traitées lorsque, dans les circonstances de l'espèce, cette personne ne peut raisonnablement s'attendre à un traitement ultérieur de celles-ci ».

Ce test est depuis lors explicitement utilisé par l'APD pour étudier cette base de licéité. Ainsi, à titre d'exemple, dans l'affaire citée précédemment concernant la communication à des commissaires sportifs des interdictions de fréquentation prononcée par le tribunal du sport[423], l'APD a considéré que, dans le cas d'espèce, les conditions dégagées par la jurisprudence européenne[424] sont remplies (tests de finalité, de nécessité, et de pondération)[425].

**93. Intérêt légitime et transparence.** La politique de confidentialité du responsable du traitement doit mentionner quelles finalités reposent sur l'intérêt légitime du responsable, tout en démontrant en quoi consisterait précisément cet intérêt légitime, le RGPD imposant cette mention à ses articles 13 et 14. Par ailleurs, l'APD a considéré qu'un responsable du traitement qui basait un transfert de données à d'autres sociétés du même groupe sur son intérêt légitime, sans expliquer en quoi celui-ci prévalait sur les droits et intérêts des personnes concernées, ne respectait pas le RGPD[426]. À cette occasion, l'APD a indiqué que, « à titre de bonne pratique, le responsable du traitement peut également, avant la collecte de données à caractère personnel de la personne concernée, fournir à cette dernière des informations sur la pondération qu'il convient de faire afin de pouvoir utiliser l'[intérêt légitime] comme fondement juridique du traitement ».

**94. Réseaux sociaux – Fonctionnalité « inviter un ami ».** Dans le cadre d'une action contre un réseau social qui avait mis en place une fonctionnalité permettant à ses membres d'inviter leurs 'amis/contacts' à rejoindre ce réseau social, l'APD, après avoir écarté la possibilité de baser ce traitement sur le consentement des personnes contactées, a jugé que l'intérêt légitime du réseau (à des fins de prospection) ne passait pas le test de pondération compte tenu des données collectées[427].

**95. Intérêt légitime comme solution subsidiaire.** Bien souvent, l'intérêt légitime est considéré par les responsables de traitements comme l'ultime solution quand il s'avère impossible de fonder un traitement sur d'autres bases de licéité. Ainsi, il n'est pas rare de voir dans les décisions de l'APD le responsable du traitement tenter de justifier, parfois *a posteriori*, le traitement sur base de son intérêt légitime. Tel était le cas dans l'affaire concernant un célèbre réseau social, citée au point précédent[428].

422 C.J., 11 décembre 2019, arrêt *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18.

423 APD, 30 juin 2020, décision n° 42/2020.

424 C.J., 4 mai 2017, arrêt *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA „Rīgas satiksme"*, C-13/16. Sur cet arrêt, nous renvoyons à notre chronique précédente *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 113 et s.

425 APD, 30 juin 2020, précité, points 28-35.

426 APD, 14 mai 2020, décision n° 24/2020.

427 APD, 14 mai 2020, décision n° 25/2020. Le réseau social en question a écopé d'une amende de 50.000 euros. Sur la qualification des acteurs et l'applicabilité de l'exception à des fins strictement personnelles, voy. *supra*, § 64.

428 *Idem*.

Dans sa décision du 30 octobre 2020 déjà évoquée[429], l'APD considère notamment que la publication d'une vidéo montrant la cheminée d'un immeuble et sa fumée, accompagnée du nom et de l'adresse de son occupant, en vue de dénoncer la pollution dégagée, ne répond pas à la condition de licéité du traitement, puisque ni l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ni l'intérêt légitime du responsable du traitement, ni le consentement de la personne concernée, ni la sauvegarde des intérêts vitaux de tiers, ne trouvent à s'appliquer en l'espèce.

Par ailleurs, dans un arrêt du 18 septembre 2018, la cour d'appel de Gand considère qu'une vidéo publiée sur *YouTube*, *Facebook*, *Vimeo* et *Twitter*, montrant de façon incidente un policier dans l'exercice de ses fonctions, ne nécessite pas d'obtenir le consentement dudit policier pour que le traitement soit licite et loyal[430]. Le raisonnement de la cour est notamment basé sur l'objectif poursuivi par la personne ayant filmé la vidéo, qui est assimilé à du journalisme *in casu*, et sur l'objet de la vidéo, qui n'est pas le policier lui-même, mais une action plus large[431].

**96. Intérêts légitimes en cas de responsabilité conjointe.** Si deux responsables du traitement sont considérés comme étant responsables conjoints d'un traitement[432], l'intérêt légitime s'apprécie dans le chef de chacun d'entre eux, au vu du traitement effectué. Dès lors, ils doivent tous les deux justifier d'un intérêt spécifique. La C.J.U.E. a clarifié ce point dans l'arrêt *Fashion-ID*, en précisant que tant le gestionnaire du site concerné par le placement du contenu de tiers (*Fashion-ID*) que le tiers qui plaçait son contenu sur ce site devaient justifier d'un intérêt propre[433].

### *6. Droits de la personne concernée*

**97. Introduction.** La période analysée a fait l'objet de nombreux recours devant l'APD, mais également devant divers cours et tribunaux belges et européens. Il en ressort que la personne concernée par le traitement de ses données à caractère personnel bénéficie d'une réelle protection et d'un soutien irréfutable de la part des autorités compétentes lorsque ses droits sont bafoués[434].

**98. Réponse à une demande d'une personne concernée – Modalités[435].** Le responsable du traitement doit fournir suffisamment d'efforts pour réagir adéquatement et de manière claire et complète aux demandes d'exercices de droits des personnes concernées. Plusieurs affaires soumises à l'APD peuvent éclairer la manière dont celle-ci applique ces critères.

Dans une affaire concernant une demande d'effacement du nom d'une personne sur un site web, l'APD confirme qu'il convient de répondre dans le délai prévu par le RGPD, mais que les mesures

429 APD, 30 octobre 2020, décision n° 71/2020.
430 Gand, 18 septembre 2018, *PenR.*, 2019, n° 1, pp. 37-40.
431 Gand, 18 septembre 2018, *PenR.*, 2019, n° 1, pp. 37-38. Il est à noter que la motivation de l'arrêt est très courte, et ne donne pas le détail du raisonnement juridique tenu par les juges néerlandophones.
432 Au sens de l'article 26 du RGPD.
433 C.J., 29 juillet 2019, arrêt *Fashion ID c. Verbraucherzentrale*, précité. Voy. à ce sujet *supra*, § 72.
434 Voy. également *supra*, § 74. Il est en effet fréquent que l'APD considère que le principe général de transparence n'a pas été respecté lorsque la réponse à une demande d'information ou d'accès n'a pas été adaptée.
435 Article 12 du RGPD.

gouvernementales prises pour lutter contre le Covid (obligation de télétravail…) pouvaient justifier qu'un délai plus long soit accordé au responsable[436].

L'APD a également rappelé[437] qu'une demande d'information complémentaire pouvait être effectuée par le responsable du traitement pour répondre à la demande, lorsque la demande n'est pas suffisamment claire ou lorsqu'il existe un doute raisonnable quant à l'identité du demandeur[438], mais encore faut-il que ce doute soit justifié. Dans le cas d'espèce, la demande d'accès avait été effectuée par l'intermédiaire d'un avocat, et non par la personne concernée elle-même, raison pour laquelle le responsable du traitement (une banque en l'occurrence) a douté de l'identité de la personne à l'origine de la demande. Néanmoins, l'APD a précisé que la banque avait mal réagi puisqu'elle « n'a pas motivé en quoi elle pouvait douter du mandat de leur conseil, avocat au barreau, de représenter des clients pas plus qu'elle n'a motivé en quoi elle pouvait douter des déclarations de cet avocat en ce qui concerne l'identité de ses clients »[439].

À cette occasion, l'APD a aussi précisé la portée du considérant 63 du RGPD, qui permet au responsable du traitement de demander à la personne concernée de préciser sa demande (« sur quelles données ou quelles opérations de traitement sa demande porte »). Elle ajoute en effet qu'en l'absence de pareille demande d'éclaircissement adressée à la personne concernée, la demande de celle-ci devait être considérée comme suffisamment claire pour la banque, qui se devait alors de répondre dans le délai légal d'un mois.

**99. Droit d'être informé[440].** Le responsable du traitement se doit d'informer la personne concernée de ses droits dans sa politique de confidentialité. Ainsi, dans la décision citée précédemment de l'APD du 14 mai 2020 au sujet de la légalité de la fonction 'inviter un ami', le réseau social n'informait pas les personnes concernées par cette demande d'invitation de la possibilité d'exercer leur droit d'opposition[441].

Par ailleurs, *Google* s'est trouvé en défaut d'identifier clairement quelle est l'entité juridique précise responsable des traitements de données réalisés dans le cadre des activités de référencement du moteur de recherches de *Google*, ce qui complique l'exercice de ses droits par la personne concernée, qui ne sait pas qui est son interlocuteur[442].

Les deux décisions reprises ici ne sont évidemment pas les seules où l'APD a considéré que la politique de confidentialité du responsable de traitement ne mentionne pas l'ensemble des éléments devant s'y trouver. En effet, il arrive régulièrement qu'au cours de l'instruction d'une plainte portant sur un autre point, le service d'inspection remarque que la politique de confidentialité n'est pas suffisamment complète. Cela s'avère en effet assez rare que ce point soit l'élément déterminent pour envoyer le dossier à la Chambre contentieuse.

436 APD, 7 août 2020, décision n° 46/2020.
437 APD, 28 avril 2020, décision n° 17/2020.
438 Article 12 du RGPD
439 D'autres éléments factuels étaient de nature à confirmer la validité du mandat de l'avocat.
440 Articles 12 et s. Voy. également *supra*, § 74. Il est en effet fréquent que l'APD considère que le principe général de transparence n'a pas été respecté lorsque la réponse à une demande d'information ou d'accès n'est pas adaptée.
441 APD, 14 mai 2020, décision n° 24/2020. Nous renvoyons au § 64 pour plus de détails.
442 APD, 14 juillet 2020, décision n° 37/2020. Voy. *supra*, § 74.

**100. Droit d'accès – Généralités.** Aux termes de l'article 15 du RGPD, la personne concernée a le droit d'obtenir du responsable de traitements la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées, ainsi que, le cas échéant, une copie de celles-ci.

Dans une affaire datant du 9 juillet 2019, le plaignant a été laissé dans l'ignorance totale lors de sa demande d'accès à son dossier personnel. Il a été considéré que le droit d'accès avait été restreint de manière disproportionnée en privant le plaignant d'informations essentielles, à savoir en ne lui donnant pas accès aux documents qui étaient à l'origine de la révocation de sa nomination. Malgré sa demande répétée, il n'a pas été informé des raisons pour lesquelles on est revenu sur la décision de le désigner en tant que membre suppléant de la Commission médicale provinciale du Limbourg[443].

Le tribunal de première instance de Bruxelles rappela également qu'un assureur, en tant que responsable du traitement des données, est tenu de transmettre à l'assuré qui le demande les données personnelles relatives à son état de santé, en ce compris notamment les rapports du médecin-conseil de l'assureur[444].

**101. Droit d'accès – Procédure adaptée.** Afin d'être le plus effectif possible, le responsable du traitement doit mettre en place une procédure spécifique en cas de demande. Dans une affaire de contestation d'une contravention de stationnement, l'APD a donc considéré comme non adaptée la réponse à une demande d'accès consistant en « un renvoi vers l'huissier de justice et une copie du rappel de paiement qu'elle contestait avoir reçu »[445]. À ces yeux, le service clientèle du responsable du traitement aurait dû renvoyer ce cas à leur DPO ou à la personne en charge de traiter les demandes de droit d'accès des personnes concernées[446].

Dans la même affaire, l'APD a également précisé que la personne concernée pouvait choisir la manière dont elle adresse sa demande au responsable du traitement. Ainsi, on ne peut lui reprocher de ne pas avoir utilisé le formulaire adéquat, même si on l'a informé de l'existence de ce formulaire, ou de s'être adressée au responsable du traitement par une autre voie (par exemple via une autre adresse e-mail que celle prévue normalement). De plus, toujours dans cette affaire, la distinction entre une procédure pour « plainte » et pour « exercice d'un droit d'accès à ses données », qui était opérée par le responsable pour orienter la personne souhaitant s'adresser à lui, a été considérée comme peu évidente par l'APD, compliquant inutilement les démarches pour les personnes concernées.

**102. Droit d'accès – Existence propre.** Dans une affaire du 29 juillet 2020, l'APD a estimé que c'était à tort que le responsable du traitement conditionnait l'exercice d'un droit d'accès à la possibilité ou à l'intention de rectifier les données personnelles auxquelles il serait accédé et/ou dont une copie serait délivrée. En effet, les données traitées peuvent être des données subjectives et ne pas nécessairement se prêter à l'exercice d'un droit de rectification. Plus fondamentalement,

443 APD, 9 juillet 2019, décision n° 5/2019. Voy. également *infra*, § 164.
444 Civ. Bruxelles, 8 octobre 2019, *TGZ*, 2020/3, pp. 256-258.
445 APD, 23 décembre 2020, décision n° 81/2020.
446 De surcroît, les coordonnées de ces personnes n'étaient pas reprises dans la politique de confidentialité, alors que cela est obligatoire.

s'il est certes la « porte d'entrée » qui permet l'exercice des autres droits que le RGPD confère à la personne concernée par le traitement de ses données personnelles, tel le droit à la rectification, le droit d'accès n'est pas conditionné par la possibilité ou le souhait de la personne concernée d'exercer ces autres droits[447].

**103. Droit à l'effacement**[448]**.** L'objet de la plainte qui a donné lieu à la décision n° 8/2019 de l'APD concernait essentiellement l'exercice du droit à l'effacement. Elle rappela que, même si le responsable du traitement ne donne pas suite à une demande d'effacement de données, il est tenu d'informer la personne concernée des raisons de son inaction (article 12.4. du RGPD). Plutôt que de déclarer qu'il n'était pas possible d'effacer les données personnelles du plaignant, le défendeur aurait dû informer le plaignant du fait que ceci était dû au fait que les données de la personne concernée n'étaient pas stockées dans son fichier de données, ce qui n'a pas été fait[449].

**104. Droit à l'oubli – Rappel de la jurisprudence belge en matière de droit à l'oubli judiciaire.** Dans un arrêt du 8 novembre 2018, la Cour de cassation a rappelé sa jurisprudence concernant l'existence d'un droit à l'oubli judiciaire en matière d'archive de presse en ligne, en se basant toujours sur l'ancienne loi du 8 décembre 1992 et sur le droit à la vie privée reconnus dans différents textes belges, européens et internationaux. La Cour a donc considéré qu'il découle de ces textes un droit à l'oubli permettant à une personne « reconnue coupable d'un crime ou d'un délit de s'opposer dans certaines circonstances à ce que son passé judiciaire ou le lien alors établi entre elle et les faits constitutifs d'infractions soient rappelés au public à l'occasion d'une nouvelle divulgation de ces faits »[450]. En l'occurrence, il s'agissait de la publication en ligne d'archives de presse initialement parues bien des années avant en version papier. Dès lors, la personne est en droit de demander qu'elle ne soit plus identifiable sur l'archive de presse publiée en ligne, même si le texte était à l'époque paru de manière parfaitement légale.

**105. Droit au déférencement et droit à l'oubli**[451]**.** Durant la période étudiée, *Google* a été mis en avant à plusieurs reprises dans des affaires liées au droit à l'oubli et au déréférencement.

La première décision qui nous intéresse concerne pour une fois, une décision de l'ordre judiciaire et non de l'APD, ce qui est assez rare pour le souligner, en particulier concernant des demandes de déréférencement. En l'occurrence, le demandeur a donc agi devant le tribunal de première instance de Bruxelles, dans le cadre d'une procédure en référé. Celui-ci souhaitait que certains articles de presse relatant différents faits de nature délictueuse, pour certains desquels il a été condamné il y a de cela plus de quinze ans, n'apparaissent plus comme résultat de recherche sur le célèbre moteur de recherche *Google*[452]. À cette occasion, le tribunal a rappelé le rôle décisif du moteur de recherche dans la diffusion globale des données à caractère personnel « en ce

447 APD, 29 juillet 2020, décision n° 41/2020.

448 Article 17 du RGPD.

449 APD, 17 septembre 2019, décision n° 8/2019.

450 Cass., 8 novembre 2018, R.G. n° C.16.0457.F. Pour une analyse plus détaillée et contextualisée de cet arrêt, voy. dans la présente chronique la partie IV « Médias, liberté d'expression et nouvelles technologies », § 234.

451 Article 17 du RGPD. Pour une analyse plus détaillée et complémentaire de ces décisions, voy. dans la présente chronique la partie IV « Médias, liberté d'expression et nouvelles technologies », §§ 223 et s.

452 Le même type de fait que dans l'affaire C.J., 13 mai 2014, arrêt *Google Spain SL Google inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12. À ce sujet, nous renvoyons à la *Chronique de jurisprudence en droit des technologies de l'information 2012*-2014, *R.D.T.I.*, 2015, n° 59-60, pp. 97 et s.

qu'il rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris aux internautes qui, autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées »[453]. Le tribunal a estimé que bien que les articles litigieux puissent être considérés comme ayant une certaine valeur historique et ayant connu un certain retentissement à l'époque, il s'agissait cependant de faits anciens remontant à près de vingt-cinq ans. Le référencement de tels articles de presse n'enrichit donc plus le débat actuel. Le tribunal conclut en soulignant que « l'intérêt de référencer ces données sur le moteur de recherche *Google* excède la durée nécessaire et ne s'impose plus historiquement »[454], et que l'exception prévue à l'article 17.3 du RGPD (traitements nécessaires à la liberté d'expression et d'information) ne voyait pas à s'appliquer ici vu que l'article initial reste accessible et que la balance des intérêts entre le droit à l'information et le droit à l'oubli de la personne penchait en faveur de cette dernière.

Dans une autre affaire, dont le défendeur se trouve être encore une fois *Google*, le demandeur se plaint du refus de *Google* de faire droit à ses demandes de déréférencement envoyées via les formulaires en ligne. Il souhaitait la suppression des liens vers de nombreux articles de la presse belge attentant à son honneur et à sa réputation et référencés dans le moteur de recherche. Compte tenu de la jurisprudence de la C.J.U.E. (voyez notamment les arrêts *Google Spain*[455], *Google/CNIL*[456] et *GC et al./CNIL*[457]), et de l'arrêt de la Cour de cassation belge du 8 novembre 2018[458], il a été considéré que dès réception du formulaire de demande de déréférencement introduit par le plaignant, Google a eu une connaissance effective du caractère ancien de la plainte pour harcèlement et que cette dernière était susceptible de porter préjudice au plaignant. La Chambre contentieuse a estimé que *Google Belgique* avait dès ce moment une connaissance effective de motifs sérieux de nature à exiger un déréférencement sur base de l'article 17.1.a) du RGPD[459].

**106. Demande de déréférencement – Cour européenne des droits de l'homme.** Dans son arrêt du 28 juin 2018, la Cour européenne des droits de l'homme a conclu à une non-violation de l'article 8 CEDH qui consacre le respect à la vie privée. L'atteinte initiale à la vie privée des requérants résultait de la décision des médias concernés de publier leurs données personnelles et de les garder disponibles sur leurs sites web, les moteurs de recherche ne faisant qu'amplifier l'atteinte. Or, la Cour estime que « les obligations des moteurs de recherche à l'égard de la personne concernée par l'information peuvent être différentes de celles de l'éditeur à l'origine de l'information. Par conséquent, la mise en balance des intérêts en jeu peut aboutir à des résultats différents selon que se trouve en cause une demande d'effacement dirigée contre l'éditeur initial

453 Civ. Bruxelles (réf.), 4 novembre 2019, *A&M*, 2018-2019/4, pp. 508-514. Sur cette décision, voy. également dans la partie IV « Médias, liberté d'expression et nouvelles technologies », § 232.

454 *Ibid.*

455 C.J., 13 mai 2014, arrêt *Google Spain SL et Google inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12.

456 C.J., 24 septembre 2019, arrêt *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17. Sur les autres enseignements de cet arrêt (champ d'application territoriale…), voy. *supra*, §§ 66 et 70, et *infra*, § 108.

457 C.J., 24 septembre 2019, arrêt *GC et al. c. CNIL*, C-136/17. Sur cet arrêt, voy. *infra*, § 107.

458 Cass., 8 novembre 2018, C.16.0457.F. Pour plus de détails à ce sujet, voy. *supra*, § 104.

459 APD,14 juillet 2020, décision n° 37/2020. Cette décision est d'autant plus intéressante à citer ici qu'elle applique explicitement les enseignements de la C.J.U.E. en matière de répartition de compétence entre autorités nationales dans le cadre de groupes de société comme Facebook, et de portée territoriale de la demande de déréférencement.

de l'information (dont l'activité se trouve en règle générale au cœur de ce que la liberté d'expression entend protéger), ou contre un moteur de recherche (dont l'intérêt principal n'est pas de publier l'information initiale sur la personne concernée, mais de permettre de repérer toute information disponible sur celle-ci et d'en établir un profil) »[460].

**107. Droit au déréférencement – Portée « territoriale ».** Depuis maintenant quelques années, l'existence d'un droit spécifique au déréférencement n'est plus contestable. Il restait cependant la question de savoir la portée exacte de ce droit ou, pour le dire autrement, à quelles extensions d'un moteur de recherche une demande de déréférencement pouvait s'appliquer.

Dans un arrêt du 24 septembre 2019[461], la C.J.U.E. a considéré que le droit au déréférencement n'avait pas à s'appliquer sur l'ensemble des extensions existantes, et se limitait uniquement aux extensions relatives aux États membres de l'Union. Afin d'éviter un contournement trop aisé de cette règle, la Cour impose également aux moteurs de recherche la mise en place « des mesures qui […] permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens [qui devraient être supprimés sur les extensions européennes du site] ».

**108. Droit au déréférencement – Données « sensibles ».** En septembre 2019, la C.J.U.E. a été appelée à se prononcer sur le champ d'application matériel des dispositions relatives aux catégories particulières de données à caractère personnel[462]. Dans cet arrêt, la Cour considère qu'un moteur de recherche doit lui aussi respecter les règles encadrant les données « sensibles », mais que, du fait de sa position d'intermédiaire important dans la diffusion de l'information, ce n'est en principe pas à lui de contrôler *a priori* qu'aucune donnée sensible ou relative à une condamnation pénale ne sera référencée. Celui-ci doit cependant tenir compte du caractère particulier de ces données lors du traitement des demandes de déréférencement. Ce droit au déréférencement n'est donc pas absolu, même pour ce type particulier de données. Les différentes exceptions au droit au déréférencement restent en effet applicables (traitement nécessaire à l'exercice du droit à la liberté d'information…)[463].

**109. Droit à la portabilité des données[464] – Dossier comptable.** Dans le cadre d'un litige concernant le transfert d'un dossier entre l'ancien comptable de la personne concernée et son nouveau comptable, le tribunal de commerce de Gand a précisé que le droit à la portabilité des données ne pouvait pas être invoqué par le nouveau comptable lui-même pour récupérer le

460 Cour eur. D.H., arrêt *M.L. et W.W. c. Allemagne*, 28 juin 2018, req. n[os] 60798/10 et 65599/10. Voy. également l'analyse de cette décision dans la partie partie IV « Médias, liberté d'expression et nouvelles technologies », §§ 196 et s.

461 C.J., 24 septembre 2019, arrêt *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL),* C-507/17. Sur les autres enseignements de cet arrêt (champ d'application territoriale…), voy. *supra*, §§ 66, 70 et 108, ainsi que dans la partie IV « Médias, liberté d'expression et nouvelles technologies », §§ 226 et s.

462 C.J. (gde ch.), 24 septembre 2019, arrêt *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17. Voy. l'analyse détaillée de cet arrêt faite *supra*, § 70, ainsi que dans la partie IV « Médias, liberté d'expression et nouvelles technologies », §§ 225 et s.

463 Voy. également l'analyse de cet arrêt dans la partie IV « Médias, liberté d'expression et nouvelles technologies » de cette chronique concernant l'équilibre entre « droit à l'oubli » et « liberté d'expression », §§ 223 et s..

464 Article 20 du RGPD.

dossier (numérique) de son client. Seul le client peut se prévaloir de ce droit[465], client qui pourrait éventuellement mandater son nouveau comptable pour l'exercer pour son compte.

**110. Droit d'opposition – Marketing direct[466].** Dans une affaire du 29 mai 2020, l'APD a analysé une plainte concernant la réception répétée par courrier de matériel promotionnel, et ce en dépit du fait que la plaignante ait demandé à plusieurs reprises au défendeur de ne plus les lui envoyer et d'effacer ses données à caractère personnel. Étant entendu qu'il s'agissait de prospection, la plaignante avait la possibilité de retirer son consentement, à tout moment et sans frais, et de s'opposer au traitement de ses données personnelles, et ce, qu'il s'agisse ou non du traitement initial ou d'un traitement ultérieur, conformément au considérant 70 du RGPD[467]. Dans le cadre d'un système de prospection, une telle opposition doit dès lors donner lieu immédiatement et sans examen supplémentaire à l'arrêt pur et simple de tout traitement de données de la personne concernée pour ces finalités de marketing direct[468]. En outre, le responsable du traitement doit faciliter ce droit d'opposition[469].

### *7. Flux transfrontières*

**111. Arrêt *Schrems II* – Rappel de l'arrêt *Schrems I* et du *Safe Harbor*.** Si la chronique précédente était marquée par le célèbre arrêt de la C.J.U.E. *Schrems I*[470], celle-ci est marquée par l'arrêt *Schrems II*, c'est-à-dire l'arrêt de la C.J.U.E. du 16 juillet 2020[471].

Dans l'arrêt *Schrems I*, la C.J.U.E. avait invalidé le système mis en place sous le nom de « Safe Harbor » qui permettait d'autoriser le transfert de données à caractère personnel vers les États-Unis, tout en garantissant un niveau de protection adéquat à ces données qui, sinon, ne seraient pas aussi bien protégées outre-Atlantique. Concrètement, ce système reposait sur une décision d'adéquation de la Commission européenne qui permettaient aux entreprises respectant volontairement certaines règles édictées dans le cadre du *Safe Harbor* de transférer des données vers les États-Unis. Dans son arrêt *Schrems I*, la Cour justifie l'invalidation de ce système par l'absence de mécanisme concret et efficace de contrôle des règles convenues dans le cadre de ce *Safe Harbor*, par la trop large possibilité laissée aux services de sécurité américains de pouvoir accéder à ces données (sans possibilité de recours effectif), et par l'impossibilité pour les autorités de contrôle nationales de pouvoir prendre des mesures afin d'assurer le respect des principes édictés dans l'accord.

À la suite de cette décision, et face à l'obligation, vu l'importance de ces flux dans le fonctionnement actuel de la société de l'information, de prévoir un nouveau mécanisme permettant le transfert de données vers les États-Unis, la Commission a rapidement renégocié un accord « similaire »,

465 Gand (div. Courtrai), 24 juillet 2018, *T.G.R.*, 2018/4, pp. 268-271 ; *R.W.*, 2019-2020/4, pp. 152-154.

466 Article 21 du RGPD.

467 APD, 29 mai 2020, décision n° 28/2020.

468 APD, 17 janvier 2020, recommandation n° 01/2020 relative aux traitements de données à caractère personnel à des fins de marketing direct, p. 53.

469 APD, 16 juin 2020, décision n° 32/2020.

470 C.J., 6 octobre 2015, arrêt *Maximilian Schrems c. Data Protection Commissioner*, C-362/14. Pour l'analyse plus détaillée de cet arrêt, nous renvoyons à la *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 119 et s. et références citées.

471 C.J., 16 juillet 2020, arrêt *Data Protection Commissioner c. Facebook, M. Schrems* e.a., C-311/18.

le *Privacy Shield*[472], accord qui devait en principe contenir davantage de garanties et répondre aux différentes critiques émises par la C.J.U.E.

**112. Arrêt *Schrems II* – Analyse de l'arrêt[473].** Non satisfait du niveau de protection assuré par le *Privacy Shield* (notamment suite à l'affaire *Snowden* qui révéla l'existence de systèmes de surveillance américains bien plus développés qu'ils ne semblaient officiellement l'être), Maximilien Schrems a introduit une plainte auprès de l'Autorité de contrôle irlandaise en vue de faire interdire les transferts de données entre *Facebook Ireland* et *Facebook Inc.* Concrètement, il a souhaité remettre en cause la décision d'adéquation de la Commission créant le *Privacy Shield* et la décision de la Commission européenne 2010/87 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers[474]. La réponse de l'APD irlandaise ne l'ayant pas satisfait, il saisit la Cour suprême irlandaise qui à son tour interrogea la C.J.U.E.[475].

Concernant la validité de la décision d'adéquation sur laquelle repose le *Privacy Shield*, la Cour a considéré que le niveau de protection assuré par ce mécanisme n'était pas « substantiellement équivalent » au niveau de protection en Europe (RGPD, art. 47 de la Charte UE…) au motif notamment que le cadre légal encadrant les programmes de surveillance mis en place par les services de renseignement états-uniens n'était pas suffisamment protecteur (atteintes disproportionnées, cadre légal trop vague, absence de contrôle juridictionnel effectif). Elle invalida donc la décision d'adéquation.

Concernant les clauses contractuelles-types prévue dans la décision 2010/87 de la Commission, la Cour a considéré que « la validité de cette décision n'est pas remise en cause par le seul fait que les clauses types de protection des données figurant dans celle-ci ne lient pas, en raison de leur caractère contractuel, les autorités du pays tiers vers lequel un transfert des données pourrait être opéré. En revanche, cette validité dépend de l'effectivité des mécanismes permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté » et le cas échéant, que les transferts de données à caractère personnel soient suspendus si ce niveau ne peut être effectivement garanti. La Cour impose donc à l'exportateur de données de s'assurer de l'effectivité des mécanismes de protection prévue dans ces clauses contractuelles types.

**113. Arrêt *Schrems II* – Conséquences de l'arrêt[476].** Cet arrêt crée une grande insécurité juridique au sujet des transferts de données à destination des États-Unis, même via un mécanisme de clauses contractuelles types. Afin de tenter de répondre à ces interrogations, l'EDPB a notamment

472 Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, *J.O.*, L 207, 1er août 2016.

473 Pour une analyse plus détaillée de cet arrêt, voy. F. Jacques, « 'Uncle Sam is watching you': retour sur les enseignements de l'arrêt *Schrems II* de la Cour de justice de l'Union européenne », *J.T.*, 2021, pp. 246 et s. Pour des réponses à des questions un peu plus concrètes, voy. également le FAQ de l'EDPB relatif à cet arrêt, 23 juillet 2020, disponible sur le site de l'EDPB.

474 Décision 2010/87/CE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, *J.O.*, L 39, 12 février 2010. Ce type de clause permet aux personnes qui s'engagent à les respecter de transférer des données vers des pays tiers (mécanisme prévu actuellement à l'article 28.7 du RGPD).

475 C.J., 16 juillet 2020, arrêt *Data Protection Commissioner c. Facebook, M. Schrems* e.a., C-311/18

476 À ce sujet, voy. le FAQ de l'EDPB sur cet arrêt, 23 juillet 2020, disponible sur le site de l'EDPB.

publié une recommandation[477] visant à proposer la mise place de mesures de protection supplémentaires afin d'assurer un niveau de protection substantiellement équivalent.

À côté de cette incertitude concernant la légalité de ces transferts, plane également une incertitude quant à la possibilité pour les autorités de protection des données, qui ne sont pas l'autorité de contrôle chef de file, d'agir en justice afin de faire cesser un transfert de données transfrontalier qui ne respecterait pas le RGPD. Dans un arrêt récent, la Cour de Justice semble le leur permettre puisqu'elle considère « qu'une autorité de contrôle d'un État membre qui, en vertu de la législation nationale adoptée en exécution de l'article 58, paragraphe 5, [du RGPD] a le pouvoir de porter toute prétendue violation dudit règlement à l'attention d'une juridiction de cet État membre et, le cas échéant, d'ester en justice peut exercer ce pouvoir en ce qui concerne un traitement de données transfrontalier, alors qu'elle n'est pas l'"autorité de contrôle chef de file", au sens de l'article 56, paragraphe 1, du même règlement, s'agissant de ce traitement de données, pour autant que ce soit dans l'une des situations où le règlement 2016/679 confère à cette autorité de contrôle une compétence pour adopter une décision constatant que ledit traitement méconnaît les règles qu'il contient ainsi que dans le respect des procédures de coopération et de contrôle de la cohérence prévues par ce règlement »[478].

### *8. Autorités de contrôle et sanctions*

**114. Litispendance entre APD et autorité judiciaire quant à la légalité d'un traitement.** Le juge de paix de Hamme a considéré que le dépôt d'une plainte auprès de l'APD concernant une collecte potentiellement illégale de données à caractère personnel dans le cadre d'une enquête visant à s'assurer du respect des conditions d'attribution de logements sociaux par la société de gestion de ces logements n'était pas de nature à empêcher la juridiction d'examiner la validité et l'admissibilité de ces données comme preuve dans cette affaire[479].

**115. Plainte auprès de l'APD – Absence d'intérêt personnel à agir.** L'APD a eu l'occasion de rappeler à plusieurs reprises que pour pouvoir introduire une plainte, la personne devait nécessaire pouvoir justifier d'un intérêt personnel à agir, faute de quoi la plainte devait être classée sans suite.

Tel était notamment le cas dans une affaire où une personne, souhaitant rester anonyme, a déposé plainte contre un carwash qui aurait placé des caméras en violation de la législation en vigueur. Ce plaignant indiquait d'ailleurs clairement qu'il n'avait aucun intérêt personnel à agir, et qu'il faisait cela seulement dans « l'intérêt public »[480]. Allant dans le même sens, l'APD a également classé sans suite une plainte dans laquelle le plaignant (un client d'un magasin) alléguait que les caméras utilisées dans un magasin (le défendeur) pourraient être utilisées pour licencier du

477 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 november 2020.

478 C.J., 15 juin 2021, arrêt *Facebook c. Gegevensbeschermingsautoriteit*, C-645/19. Cette affaire est la suite de l'affaire *Facebook* dans laquelle l'APD belge avait agi en justice pour leur interdire certains traitements de données (voy. *supra*, § 65). Cette décision de la Cour sera analysée dans la prochaine chronique.

479 JP Hamme, 6 juin 2019, *J.J.P.-T.Vred.*, 2020/1, pp. 122-131.

480 APD, 17 décembre 2020, décision n° 80/2020. À cette occasion, l'APD a également rappelé dans quel cas un plaignant pouvait rester anonyme (art. 47 du ROI de l'APD).

personnel de ce magasin. L'APD considéra que le plaignant n'étant pas lui-même un employé du magasin, il n'avait aucun intérêt personnel à agir[481].

**116. Opportunité d'action – Infraction RGPD accessoire**. Dans une affaire concernant une publicité ciblée mensongère (la société se présentant comme une ASBL et non comme une entreprise commerciale), l'APD a classé sans suite la plainte de la personne ayant été soumise à cette publicité ciblée au motif que mentir sur l'identité de l'entité derrière cette publicité était avant tout un problème de publicité trompeuse et non un problème de protection des données (violation de certaines règles en matière de transparence…), et qu'enquêter sur ce type de pratique n'entrait donc pas dans les priorités de l'APD[482].

**117. Condamnation pénale d'un responsable du traitement.** Même si la sanction la plus fréquente suite à la violation des règles en matière de protection des données reste une condamnation à une amende administrative par l'APD, il arrive parfois que le responsable du traitement soit poursuivi, et condamné, pénalement. Ainsi, une société de distribution d'eau a écopé d'une amende pénale de 600 EUR[483] pour avoir violé certaines règles du RGPD dans le cadre d'une procédure de constatation de facture d'eau, facture qui était adressée à la mauvaise personne. La société aurait agi avec une négligence grave en ne répondant pas aux demandes de la personne contestant la facture, qui souhaitait pouvoir avoir accès à ces données de facturation afin de les faire corriger[484].

**118. Répartition de compétence entre autorités de contrôle nationales et droit applicable.** Dans l'affaire *Wirtschaftsakademie* précédemment citée[485], la C.J.U.E. devait notamment répondre à la question de savoir si, dans le cas où le droit applicable est son droit national (le droit allemand *in casu*), une autorité de contrôle d'un État membre (l'ULD) doit nécessairement passer par une demande à l'autorité du pays où est établi le responsable du traitement (l'autorité de contrôle irlandaise) avant d'agir, ou si elle peut agir directement.

La Cour a largement suivi les conclusions de l'avocat général Bot en affirmant que lorsqu'une entreprise établie en dehors de l'Union européenne (*Facebook Inc.*) dispose de plusieurs établissements dans différents États membres (une filiale dans chaque pays), l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de la directive 95/46 à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre (*Facebook* avait un établissement en Allemagne[486]). Cela signifie que la répartition officielle des missions entre les différentes entités juridiques au sein d'un groupe (*Facebook*) n'est pas pertinente pour exclure la compétence de certaines autorités de contrôle nationale. En l'occurrence, l'autorité de contrôle allemande est donc compétente puisqu'est établi sur son territoire

481 APD, 13 mai 2020, décision n° 23/2020. L'APD doute également de l'existence réelle de pareil traitement des données venant des caméras de surveillance.

482 APD, 22 septembre 2020, décision n° 65/2020. Voy. plan Stratégique 2020-2025 de l'APD, disponible sur son site web.

483 À majorer des décimes additionnels.

484 Mons, 15 janvier 2020, *J.T.*, 2020/30, pp. 613 et s., et note de N. Roland.

485 C.J., 5 juin 2018, arrêt *Wirtschaftsakademie Schleswig-Holstein*, C-210/16. Voy. *supra*, § 72.

486 Sur la notion d'établissement, voy. C.J., 1er octobre 2015, arrêt *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14. Une analyse de cet arrêt, en lien avec l'arrêt *Wirtschaftsakademie Schleswig-Holstein*, était déjà proposée dans la *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 100 et s.

*Facebook Germany*, quand bien même cette entité n'est chargé que de la vente d'espaces publicitaires et d'autres activités de marketing sur ce territoire et que la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union européenne, à un établissement situé dans un autre État membre (l'Irlande)[487]. L'autorité allemande peut donc agir de manière autonome, sans forcément demander l'avis d'une autorité d'un autre État membre.

**119. Déréférencement en cours de procédure devant la Chambre contentieuse de l'APD.** Suite à un refus de supprimer un lien sur le moteur de recherche de *Google*, une plainte auprès de l'APD a été introduite. Cependant, en pleine action devant la Chambre contentieuse de l'APD, les parties se sont concertées et se sont mises d'accord sur les liens à déréférencer, sans faire intervenir la Chambre. Cette dernière a néanmoins considéré que, bien que les parties soient parvenues à un arrangement, elle demeurait habilitée à examiner la licéité des motifs de refus initial du droit à l'effacement. Elle justifie sa décision par le fait qu'il suffirait pour les responsables du traitement de ne donner suite aux demandes d'exercice des droits des personnes concernées qu'au stade de la procédure pour être ainsi exemptés de toute violation antérieure[488].

## B. Questions spéciales concernant les communications électroniques

### *1. Communication électronique et rétention de données*[489]

**120. Obligations de conservation de données – Rappel général.** Suite à l'annulation de l'article 126 de la loi relative aux communications électroniques (ci-après LCE) par la Cour constitutionnelle en 2015[490], le législateur a voté une nouvelle version, peu éloignée de l'ancienne, de l'article en 2016. Il imposait donc aux « fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'internet, de courrier électronique par internet [,aux] opérateurs fournissant des réseaux publics de communications électroniques ainsi qu['aux] opérateurs fournissant un de ces services » une obligation de conserver les données générées ou traitées par eux « pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé », tandis que l'article 9, § 7, de la LCE imposait des obligations similaires aux « fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public ».

**121. Arrêt *Quadrature du net* – Rappel et affinement de la jurisprudence de la C.J.U.E.** En réponse à des questions préjudicielles venant notamment de la Cour constitutionnelle belge qui doit de nouveau traiter d'un recours en annulation portant notamment sur la nouvelle version de l'article 126 de la LCE[491], la C.J.U.E. a rappelé[492] que l'article 15, paragraphe 1, de la directive « vie

487 C.J., 5 juin 2018, arrêt *Wirtschaftsakademie Schleswig-Holstein*, précité, point 64.

488 APD, 22 septembre 2020, décision n° 63/2020.

489 Certaines décisions pouvant être en lien avec ce thème se trouvent également dans la partie VI « Criminalité informatique », §§ 319 et s.

490 Pour une analyse plus détaillée de ces arrêts, nous renvoyons à la *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 12 et s.

491 C.C., 19 juillet 2018, n° 96/2018.

492 Dans le droit fil des arrêts *Digital Rights Ireland* (C.J., 8 avril 2014, aff. jointes C-293/12 et C-594/12) et *Tele2 Sverige* (C.J., 21 décembre 2016, arrêts *Tele2 Sverige AB*, C-203/15 et *Secretary of State for the Home Department*, C-698/15

privée et communications électroniques »[493], lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, §1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, § 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation[494].

En revanche, la Cour admet trois catégories d'exceptions à cette interdiction générale, dont une nouvelle par rapport à la jurisprudence antérieure : la menace grave actuelle ou prévisible à la sécurité nationale. En présence d'une telle menace, les États membres peuvent ordonner la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation pour une durée limitée. Cependant, la décision prévoyant cette injonction doit faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant. Ce contrôle doit viser à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues. De plus, ladite injonction ne peut être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace. Enfin, la Cour indique que peut se justifier :

1. pour la sauvegarde de la sécurité nationale, la lutte contre la criminalité et la sauvegarde de la sécurité publique, une obligation de conservation généralisée et indifférenciée de l'identité civile des personnes concernées ;
2. pour la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique :
   a. une conservation préventive, généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;
   b. une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;
   c. pour une durée déterminée, la conservation rapide des données relatives au trafic et des données de localisation, dont disposent ces fournisseurs de services de communications, « et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées ainsi que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée »[495].

aff. jointes). Pour une analyse plus détaillée de ces arrêts, nous renvoyons à la *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, pp. 128 et s.

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

494 C.J. (gde ch.), 6 octobre 2020, arrêt *La Quadrature du Net e.a. c. Premier ministre e.a.*, aff. jointes C-511/18, C-512/18 et C-520/18.

495 *Idem*, point 168.

En ce qui concerne les hébergeurs de sites web, la Cour estime qu'ils ne peuvent plus être contraints par la loi à surveiller pour le compte des États membres l'ensemble de leurs utilisateurs, en gardant en mémoire qui publie quoi, avec quelle adresse IP, quand, etc.[496].

Par conséquent, si les États membres peuvent toujours obliger les fournisseurs d'accès à internet à conserver les adresses IP de toute la population, ces adresses ne peuvent plus être utilisées que dans le cadre des enquêtes sur la criminalité grave ou dans les affaires de sécurité nationale. Le concept de 'menace grave pour la sécurité nationale' n'est toutefois pas harmonisé. Par exemple, en France, le Conseil d'État[497] comprend cette notion de façon large et y inclut l'espionnage économique[498] ou l'organisation de manifestations non déclarées[499]. D'autre part, le Conseil d'État français estime que la 'conservation ciblée' permise par la Cour ne peut être mise en œuvre pour des raisons matérielles et qu'elle, « à la supposer techniquement possible, présenterait un intérêt opérationnel particulièrement incertain, dès lors qu'elle ne permettrait pas, y compris en cas de faits particulièrement graves, d'accéder aux données de connexion d'une personne suspectée d'une infraction qui n'aurait pas été préalablement identifiée comme étant susceptible de commettre un tel acte »[500], justifiant ainsi le maintien d'une obligation de conservation généralisée.

**122. Annulation de la loi du 29 mai 2016 par la Cour constitutionnelle belge.** Contrairement au Conseil d'État français, la Cour constitutionnelle belge a annulé une large partie de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (loi qui réintroduisait notamment la nouvelle version de l'article 126 de la LCE), estimant que cette loi violait le droit de l'Union, en ce qu'elle prévoit, par principe et sans limitation aux hypothèses décrites par la C.J.U.E., une conservation généralisée et indifférenciée, par les opérateurs et fournisseurs de services de communications électroniques, des données d'identification, des données d'accès et de connexion, ainsi que des données de communication[501].

**123. Fourniture d'accès aux autorités nationales à des fins d'enquête.** L'article 1er, paragraphe 3, de la directive 2002/58 exclut du champ d'application de celle-ci les activités de l'État

496 « L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services », C.J. (gde ch.), 6 octobre 2020, arrêt *La Quadrature du Net e.a. c. Premier ministre e.a.,* point 212.

497 C.E. (fr.), 21 avril 2021, décision nos 393099, 394922, 397844, 397851, 424717 et, 424718, *La Quadrature du Net et autres et de l'association Igwan.net.*

498 C.E. (fr.), décision du 21 avril 2021, précité, p. 20.

499 « Le Conseil d'État cite l'article L811-3 du Code de la sécurité intérieure (CSI) qui est très très large. Il inclut des choses qui, selon nous, ne devraient pas compter comme menace grave à la sécurité nationale. Y sont cités la protection des engagements européens (difficile de savoir ce que ça veut dire exactement), l'espionnage économique, la surveillance des mouvements sociaux, la prévention des violences collectives, c'est-à-dire en fait surveiller des Gilets jaunes… », B. Lion, « Conservation des données : pour la Quadrature du Net, la France est "le seul pays à avoir à ce point tordu la décision de la C.J.U.E." », 28 avril 2021, disponible sur https://www.lesnumeriques.com/vie-du-net/conservation-des-donnees-pour-la-quadrature-du-net-la-france-est-le-seul-pays-a-avoir-a-ce-point-tordu-la-decision-de-la-C.J.U.E.-n163067.html.

500 C.E. (fr.), 21 avril 2021, précité, p. 23.

501 C.C., 22 avril 2021, R.G. no 57/2021, B.15.

dans les domaines qui y sont visés, parmi lesquelles figurent les activités de l'État dans le domaine pénal et celles concernant la sécurité publique, la défense et la sûreté de l'État, y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État.

Toutefois, le traitement de données détenues par les fournisseurs de services de communications électroniques, en vue de leur communication aux autorités judiciaires, n'est pas une activité liée à la sûreté de l'État, mais une activité de fournisseurs de services régie par cette directive. En vertu de l'article 15 de ladite directive, les États membres peuvent limiter la portée de la protection des données personnelles prévue par la directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. La Cour précise à cet égard que « l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, tel que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés [aux articles 7 et 8] de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave »[502]. En revanche, la législation européenne s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement[503].

### *2. Législation spécifique en matière de cookies*

**124. Introduction.** Il existe de nombreuses manières de tracer les utilisateurs d'un site web sur les différentes pages qu'ils consultent, mais la plus fréquente reste l'installation d'un cookie sur leur machine. Cette technologie est très répandue actuellement sur le web. Durant la période couverte par cette chronique, deux décisions ont particulièrement fait parler d'elles, à savoir l'arrêt *Planet49* de la Cour de justice[504] et une décision de l'APD du 17 décembre 2019[505]. À travers ces deux décisions, nous pourrons faire le point sur les principales particularités du cadre règlementaire encadrant l'exploitation de cookies. Ce cadre ne se limite en effet pas au RGPD, mais intègre également la directive « ePrivacy »[506].

Dans l'affaire *Planet49*, il était question d'un site web qui organisait un concours. Pour participer à ce concours, il fallait obligatoirement remplir un formulaire d'inscription qui contenait notam-

502 C.J. (gde ch.), 2 octobre 2018, arrêt *Ministerio Fiscal*, C-207/16.

503 C.J., 6 octobre 2020, arrêt *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e.a.*, C-623/17.

504 C.J., 1er octobre 2019, arrêt *Bundesverband der Verbraucherzen-tralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV c. Planet49 GmbH*, C-673/17.

505 APD, 17 décembre 2019, décision n° 12/2019.

506 Directive 2002/58 ou directive « vie privée et communications électroniques ». Cette directive est en cours de révision depuis de nombreuses années. Nous nous contenterons donc d'analyser la situation au regard du cadre légal actuel. Pour une étude plus détaillée de ces deux arrêts, nous renvoyons à A. Delforge, « Le placement de "cookies" sur un site web : la Cour de justice fait le point, l'APD commence à sanctionner », *R.D.T.I.*, 2020/1-2, pp. 101-112.

ment une case précochée (pouvant être décochée), mentionnant que le candidat acceptait le placement d'un cookie sur sa machine, et une seconde case qui, elle, devait obligatoirement être cochée par le candidat. Cette seconde case indiquait que le candidat autorisait la transmission des informations récoltées via ce formulaire à des partenaires du site, à des fins publicitaires.

L'affaire belge, quant à elle, est des plus banales puisqu'il s'agissait d'un site web d'informations juridiques, utilisant quelques cookies de tracing, qui ne respectait pas toutes les règles pour pouvoir en installer sur les ordinateurs de ses visiteurs.

**125. Applicabilité de l'article 129 de la LCE – Données à caractère personnel.** Interrogée sur la question, la C.J.U.E. précisa que l'obligation d'obtenir un consentement avant de placer un cookie « non essentiel »[507] ne dépendait pas du fait que les données contenues dans le cookie soient ou non des données à caractère personnel. Cette obligation s'applique dans les deux cas[508].

**126. Consentement RGPD et consentement ePrivacy.** S'il existe d'autres bases de licéité que le consentement dans le RGPD pour légitimer un traitement, le placement d'un cookie requiert, en vertu de la législation ePrivacy, un consentement, sauf lorsque ce cookie intervient uniquement pour des aspects purement techniques (« cookie essentiel »). Dans sa décision du 17 décembre 2019, l'APD a clairement rappelé qu'il n'était pas possible de revendiquer un intérêt légitime pour légitimer le placement de cookies à des fins statistiques[509].

Dans ses deux décisions précitées[510] du 7 décembre 2020, rendues à l'encontre de *Google* et d'*Amazon*, la CNIL a, quant à elle, jugé que ces deux géants du net avaient placé des *cookies* publicitaires sur les ordinateurs des utilisateurs de leur site résidant en France, sans consentement préalable. En effet, elle précise que ces *cookies* « n'ont pas pour finalité exclusive de permettre ou de faciliter la communication par voie électronique ni ne sont strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur »[511].

**127. Cookies – Transparence.** De par la manière dont les cookies sont installés discrètement lors de la consultation d'une page, il s'avère important que le gestionnaire d'un site indique clairement quel type de cookies peut être installé. À cet égard, la Cour de justice[512] a clairement rappelé que doivent notamment être communiqués : l'identité et les coordonnées du responsable du traitement, la finalité du traitement, les destinataires éventuels de ces données, les catégories de données collectées, l'existence de certains droits pour la personne concernée, la durée du traitement, etc.[513].

507 Sur cette notion, voy. le point suivant.
508 C.J., 1er octobre 2019, arrêt *Planet49*, précité, point 68.
509 APD, 17 décembre 2019, décision n° 12/2019.
510 Voy. *supra*, § 77.
511 CNIL, *Google LLC and Google Ireland Limited*, 7 décembre 2020, précité, § 100 ; CNIL, *Amazon Europe Core*, 7 décembre 2020, précité, § 88. Voy. *supra*, § 77. La CNIL reprend là la définition exacte, telle qu'inscrite à l'article 3 de la directive 2002/58, de « cookies essentiels ».
512 C.J., 1er octobre 2019, arrêt *Planet49*, précité.
513 Article 13 du RGPD.

Ces informations doivent également être communiquées de manière compréhensible pour la personne concernée. Ainsi, la langue employée doit correspondre à celle du service proposé, ou du public cible (et pas l'anglais, par pure facilité[514]).

**128. Consentement – Cases précochées.** Pour être valable, le consentement doit être donné clairement, ce qui ne peut être le cas lors qu'il est obtenu au moyen de cases précochées, misant ainsi sur l'inaction de la personne concernée. Ce type de pratique reste pourtant fréquente, malgré ces deux récentes décisions qui ont clairement rappelé l'importance de cette règle. Dans ses conclusions à l'occasion de l'arrêt *Planet49*, l'avocat général Szpunar va même un cran plus loin, puisqu'il recommande qu'on ne puisse pas intégrer dans un formulaire d'inscription (à un concours, ou d'accès à un service, par exemple) une demande de consentement pour le placement de cookies. Selon lui, il serait préférable que cela soit présenté de manière bien distincte pour davantage faire comprendre à la personne concernée ce qu'elle s'apprête à accepter[515].

**129. Cookies – Consentement libre.** L'obligation de cocher une case pour participer au concours, ou obtenir un service, et donc obligatoirement accepter que certaines données soient transmises à des tiers, n'est pas non plus une pratique « acceptable »[516]. En effet, elle est de nature à forcer la personne à accepter ce type de traitement, faute de quoi, elle ne peut participer au concours, accéder au site, etc. Il convient cependant de noter que la Cour ne semble pas être aussi critique que l'est l'avocat général Szpunar dans ses conclusions à l'égard de la légalité de pareilles pratiques.

### C. Questions spéciales concernant la loi « caméra »

**130. Cadre légal.** L'utilisation de caméras de surveillance est encadrée tant par le RGPD que la loi « caméra » (loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance). Si la majorité des règles sont en réalité déjà contenues dans le RGPD, la loi caméra précise certains points et impose quelques obligations supplémentaires dans le cas d'utilisation d'une caméra de surveillance orientée vers certains lieux particuliers[517]. Nous reviendrons ici sur quelques affaires portant spécifiquement sur l'utilisation de caméras de surveillance.

**131. Applicabilité de la loi « caméra » – Finalité de surveillance.** Dans une affaire concernant l'installation d'une caméra cachée dans les toilettes d'un garage afin de pouvoir espionner les personnes allant dans celles-ci[518], la Cour de cassation[519] a confirmé le raisonnement de la cour d'appel de Liège, qui avait considéré qu'il ne pouvait être reproché à la personne ayant installé cette caméra une violation des règles prévues dans la loi « caméra », dans la mesure où la caméra

514 APD, 17 décembre 2019, décision n° 12/2019.

515 Points 89 et 90 de ses conclusions.

516 La légalité de pareilles pratiques est régulièrement remise en cause, mais celles-ci ne sont qu'assez rarement formellement condamnées. À ce sujet, voy. les références citées par A. Delforge, « Le placement de "cookies" sur un site web : la Cour de justice fait le point, l'APD commence à sanctionner », *op. cit.*, pp. 108 et s.

517 Articles 2 et 3 de la loi « caméra ». Concernant l'utilisation de caméra à des fins de surveillance dans le cadre d'une relation de travail, nous renvoyons *infra*, §§ 153 et s.

518 Faits pour lesquels la personne avait été poursuivie pour attentat à la pudeur en vertu de l'article 373 du Code pénal, mais la cour d'appel, suivie par la Cour de cassation, a considéré que l'installation d'une caméra cachée ne pouvait juridiquement être qualifiée d'attentat à la pudeur, vu l'absence de contact entre la victime et la personne ayant installé la caméra.

519 Cass., 17 janvier 2018, R.G. n° P.17.0403.F/5.

installée n'est pas une caméra de *surveillance*[520] et ne rentre donc pas dans le champ d'application de la loi « caméra ».

**132. Applicabilité du RGPD – Exception à des fins strictement personnelles ou domestiques.** Dans sa décision du 24 novembre 2020, l'APD a rappelé qu'il est possible que l'utilisation de caméras puisse bénéficier de l'exception à des fins strictement personnelles ou domestiques[521]. Néanmoins, cette exception n'est pas applicable lorsque « le système de vidéosurveillance couvre par exemple l'espace public ou le domaine privé d'autres personnes, même en partie, et qu'il dépasse ainsi la sphère privée des personnes qui traitent des données au moyen de ce système »[522]. Ainsi, l'installation de caméras sur sa propriété, mais qui permettent de filmer les activités de voisins ne peut bénéficier de l'exception à des fins strictement personnelles ou domestiques et doit donc notamment reposer sur une base de licéité valable[523].

**133. Espace commun filmé – Accès aux images et responsable du traitement.** À l'occasion d'une affaire concernant le contrôle des caméras de surveillance placées dans certains espaces communs d'une résidence communautaire, l'APD a été amené à interdire à un employé de la société qui avait été chargée de la construction du bâtiment, et de l'installation des caméras, de continuer à accéder aux images, alors que le transfert de propriété avait déjà eu lieu. L'APD a donc interdit tout traitement des données par cet employé et suspendu temporaire l'utilisation de ces caméras tant que le syndicat de copropriété n'avait pas pris de décision quant à l'avenir de ces caméras[524].

**134. Espace commun filmé – Consentement des propriétaires/locataires.** Si l'on peut comprendre l'intérêt de placer dans certains espaces communs des caméras de surveillance, encore faut-il que les personnes vivant dans ces lieux y consentent. L'APD a donc logiquement estimé que « le simple fait d'installer une caméra de surveillance dans un espace commun [, à savoir la cuisine commune d'un appartement composé de kots étudiant,] où les habitants n'ont pas le choix de ne pas y pénétrer – parce que l'accès à cet espace est tout simplement nécessaire – suffit pour décider qu'une infraction à l'article 5.1.c) du RGPD [est établie] », même si l'existence de cette caméra était mentionnée clairement dans le contrat de location[525].

Dans le même sens, l'APD a également considéré que la mention dans le règlement d'ordre intérieur, applicable au moment de l'achat d'un appartement, de l'installation de caméras dans les parties communes d'un bloc d'appartement ne pouvait être considérée comme une forme de consentement libre[526].

---

520 À savoir une caméra ayant pour finalité « prévenir, constater ou déceler des infractions contre les personnes ou les biens » (art. 3,1°, de la loi « caméra »).

521 APD, 24 novembre 2020, décision n° 74/2020.

522 *Idem*. L'APD fait alors explicitement application de la jurisprudence *Rynes* (C.J., 11 décembre 2014, arrêt *František Ryneš c. Úřad pro ochranu osobních údaju*, C-212/13). Sur cet arrêt, voy. *Chronique de jurisprudence en droit des technologies de l'information 2012-2014*, *R.D.T.I.*, 2015, n° 59-60, p. 89.

523 Ce qui faisait défaut dans le cas d'espèce vu que les voisins n'avaient pas consenti, et qu'aucun intérêt légitime du défendeur ne pouvait être suffisant pour contrebalancer l'intrusion dans la vie privée de ses voisins.

524 APD, 9 juillet 2020, décision n° 36/2020.

525 APD, 2 avril 2019, décision n° ANO 03/2019.

526 APD, 9 juillet 2020, décision n° 36/2020, précitée au point précédent.

## D. Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée (K. Rosier)

**135. Contexte de la jurisprudence analysée**. La présente section propose un aperçu de la jurisprudence dans le contexte d'une prise de connaissance et d'une utilisation par un employeur de données de communications électroniques, d'images de vidéosurveillance ou de données de *tracking* issues de la géolocalisation, ainsi que de l'enregistrement de conversations électroniques et de données publiées sur un réseau social. Le sort des preuves obtenues irrégulièrement, en violation des normes applicables, est également envisagé sous la section 8.

### *1. Contrôle et prise de connaissance de communications électroniques*

**136. Cadre légal.** La prise de connaissance de courriers électroniques par l'employeur reste régie par plusieurs textes légaux, d'ailleurs régulièrement rappelés dans les décisions commentées. Le RGPD entré en application depuis le 25 mai 2018 est encore peu appliqué en jurisprudence, à l'exception des décisions rendues par l'APD, mais qui n'ont pas porté durant la période analysée sur un contrôle ou une prise de connaissance d'un message d'un travailleur par l'employeur. Ce sont donc les principes et balises issues de la protection du droit au respect de la vie privée[527] tels qu'interprétés par la Cour européenne des droits de l'homme, les dispositions particulières relatives aux communications électroniques[528], ainsi que la CCT n° 81[529] qui sont mobilisés pour arbitrer la question de la régularité de l'obtention des preuves soumises dans le cadre des litiges[530]. À l'instar des précédentes chroniques, on constate des appréciations diverses tant en ce qui concerne les normes privilégiées lors de l'analyse[531], que lors de l'examen des conséquences d'une irrégularité sur le sort de la recevabilité de la preuve[532].

**137. Loi sur les communications électroniques – Caractère intentionnel de la prise de connaissance.** Dans son arrêt du 22 février 2018, la Cour du travail de Bruxelles examinait la question de la régularité du contrôle d'une boîte mail d'un travailleur[533]. La particularité de ce contrôle était que l'employeur invoquait avoir pu prendre connaissance de courrier électronique du travailleur en vertu d'un partage des e-mails au sein d'une boîte mail dans laquelle une copie de l'ensemble des e-mails des travailleurs reçus et adressés était sauvegardée. La Cour conclut à l'existence d'une violation de l'article 124 de la loi sur les communications électroniques (ci-après LCE), en pointant en particulier le fait qu'il y a bien eu la recherche de la prise de connaissance

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

528 L'article 124 de la loi du 13 juin 2005 sur les communications électroniques.

529 Convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques.

530 Voy. not. C. trav. Liège, 13 septembre 2017, R.G. n° 2016/AU/32, disponible sur www.terralaboris.be, commenté dans *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, p. 133.

531 La Cour du travail de Liège, après avoir analysé un contrôle sous l'angle de la CCT n° 81 et rappelé l'applicabilité de l'article 8 de la CEDH en matière de contrôle des e-mails privés ou professionnels échangés via une messagerie professionnelle et les principes repris dans l'arrêt *Bărbulescu*, a estimé que l'article 124 de la loi du 13 juin 2005 offrait le cadre juridique le plus adéquat pour assurer une protection effective du droit garanti par l'article 8 (C. trav. Liège, 14 septembre 2020, R.G. n° 2019/AL/133, disponible sur www.terralaboris.be).

532 Voy. *infra*, §§ 157 et s.

533 C. trav. Bruxelles, 22 février 2018, R.G. n° 2015-AB-438, *Sem. soc. /Soc. Week*., 2018/36.

de courrier électronique ciblé démontrant l'existence d'un élément intentionnel dans le chef de l'employeur.

**138. Loi sur les communications électroniques – Exigence d'un consentement des parties à la communication**. Dans un arrêt du 20 mai 2019, la Cour de cassation relève que l'article 124 de la LCE ne distingue pas selon que les courriels aient un caractère privé ou professionnel[534]. Elle constate que l'employeur ne peut sans l'accord du travailleur prendre connaissance des courriers électroniques, et ce même s'ils ont été adressés ou reçus à partir de l'équipement de l'employeur mis à disposition du travailleur à des fins professionnelles et s'ils ne contiennent pas d'information privée, mais exclusivement des informations professionnelles.

Même avant le prononcé de cet arrêt, plusieurs décisions ont appliqué ce principe dans le cadre de l'examen de la licéité de l'obtention de courriers électroniques, et ont considéré comme irrégulière la prise de connaissance de courrier sans l'obtention du consentement du travailleur, dont la preuve incombe à l'employeur. Les juridictions saisies ont eu l'occasion d'affirmer que des décisions ou règlements unilatéraux ne suffisent pas à établir le consentement du travailleur, qui plus est lorsque ces règlements n'abordent pas la question du contrôle, mais principalement des règles de partage des e-mails[535] ou des règles concernant l'usage des ressources électroniques à des fins privées[536].

**139. Destinataire secondaire d'une communication électronique**. Durant la période examinée, plusieurs décisions se sont penchées sur la licéité de la prise de connaissance d'une communication électronique suite à une retransmission de la communication par un destinataire originaire de la communication[537]. Dans une décision du 16 janvier 2020, le tribunal du travail de Liège rappelle que si les courriers électroniques bénéficient d'une protection, cela ne fait pas obstacle à ce que le destinataire qui en a légitimement pris connaissance en communique le contenu à un tiers. Si l'expéditeur estime que le destinataire a commis, en partageant cet e-mail, une faute civile (violation du droit au respect de la vie privée ou au secret de la correspondance), voire pénale (une violation du secret professionnel, par exemple), il lui est loisible de se retourner contre cet expéditeur, mais cela n'empêche pas la régularité la prise de connaissance de la communication par le tiers à qui elle été communiquée[538].

Dans le même sens, mais à propos d'un SMS, la Cour du travail de Liège rappelle que si les communications par SMS sont couvertes par le secret des communications découlant de l'article 124 de la LCE, le fait que l'employeur ait pris connaissance par l'intermédiaire d'une des deux parties à la communication (vraisemblablement communiqué par le destinataire en réalisant une capture de l'écran de son téléphone) ne viole pas cette disposition[539]. La Cour conclut, par ailleurs, à l'absence de violation de l'article 8 de la CEDH, dans la mesure où l'expéditeur d'un SMS ne pouvait nourrir

534 Cass., 20 mai 2019, R.G. n° S.17.0089.F, *Ius & Actores*, 2019/3, pp. 459-461 ; *J.L.M.B.*, 2020, liv. 10, pp. 443 et s. ; *Ors.*, 2020 (reflet B. Paternostre), liv. 2, p. 21 ; *Chron. D.S.*, 2020, liv. 2, p. 54, concl. J. Genicot, et note S. Gilson.

535 C. trav. Bruxelles, 22 février 2018, R.G. n° 2015-AB-438, *Sem. soc. /Soc. Week.*, 2018/36.

536 C. trav. Bruxelles, 8 février 2019, *J.T.T.*, 2019/18, pp. 321-324 ; C. trav. Liège, 7 mai 2019, R.G. n° 2018/AL/128, *Chron. D.S.*, 2020, liv. 8-9, p. 359.

537 Concernant la prise de connaissance de communications par un destinataire en copie cachée, voy. C. trav. Bruxelles, 22 février 2018, R.G. n° 2015-AB-438, *Sem. soc. /Soc. Week.*, 2018/36.

538 Trib. trav. Liège, 16 janvier 2020, *RDJP*, 2020, p. 222.

539 C. trav. Liège, 24 avril 2019, R.G. n° 2018/AU/12, *Chron. D.S.*, 2020, liv. 8-9, p. 356.

des attentes raisonnables quant au fait que ce que le message ne serait pas communiqué à l'employeur par le destinataire (autre travailleur), d'autant qu'en l'espèce une partie du message visait spécifiquement une question relative à l'exécution du contrat de travail.

**140. CCT n° 81 — Champ d'application.** La Cour du travail de Gand a rappelé que la CCT n° 81 continue de s'appliquer à la prise de connaissance de communications échangées par le travailleur via sa messagerie professionnelle, même après que le contrat de travail a pris fin[540]. Dans une autre affaire dans laquelle l'employeur invoquait que la CCT n° 81 n'était pas applicable, dans la mesure où il ne s'agissait pas d'un contrôle, mais d'une prise de connaissance possible à travers le partage de communication au sein d'un service (boîte mail reprenant copie des messages envoyés et reçus des membres d'un service), la Cour du travail de Bruxelles a estimé que la convention trouvait à s'appliquer dès lors que ce mécanisme avait permis dans les faits un contrôle des courriers électroniques du travailleur produits aux débats[541].

Dans un arrêt du 8 février 2019, la Cour du travail de Bruxelles a estimé que la CCT n° 81 n'est pas applicable lorsque ce qui est reproché à l'employeur est la prise de connaissance du contenu de la communication et non des données de communication (qui sont pourtant indissociables)[542]. La Cour se réfère donc au champ d'application de la convention collective de travail qui effectivement ne concerne que les contrôles des données de communications électroniques. Elle poursuit toutefois en précisant que, ce n'est pas parce que la CCT n° 81 n'est pas applicable à la prise de connaissance du contenu des communications, que cette dernière n'est pas réglementée. Elle se réfère à l'application à cet égard à l'article 8 de la CEDH et à l'article 124 de la LCE.

**141. CCT n° 81 – Finalité du contrôle.** Il a été jugé qu'un contrôle fondé sur des soupçons à propos du comportement d'un travailleur n'entre pas dans les finalités prévues au sein de la CCT n° 81 et ne justifie certainement pas une individualisation des données de cette personne alors que l'employeur n'a pas procédé à un contrôle global qui aurait pu, si des anomalies avaient été révélées, se poursuivre par un contrôle pour une finalité admise par la CCT en respectant les modalités liées à l'individualisation correspondant à ladite finalité[543].

**142. CCT n° 81 – Caractère proportionné du contrôle.** Dans un arrêt du 7 mai 2019, la Cour du travail de Liège rappelle l'ensemble des dispositions applicables en cas de contrôle d'une adresse mail professionnelle d'un travailleur et évoque dans ce cadre également l'application de la jurisprudence issue de l'arrêt *Bărbulescu* de la Grande Chambre de la Cour européenne des droits de l'homme[544]. Elle constate que le principe de proportionnalité n'a pas été respecté en l'espèce, dès lors que l'employeur a relevé les courriels privés sans se limiter au contrôle des données de communication, et qu'il a pris connaissance du contenu des courriels « en totale contravention avec la CCT n° 81 qui ne déroge pas aux principes fondamentaux applicables en matière de protection de la vie privée, en particulier, le secret des communications »[545].

---

540 C. trav. Gand, 8 juin 2018, *R.W.*, 2020-2021/4, pp. 145-146.

541 C. trav. Bruxelles, 22 février 2018, R.G. n° 2015-AB-438, *Sem. soc. /Soc. Week.*, 2018/36.

542 C. trav. Bruxelles, 8 février 2019, *J.T.T.*, 2019/18, pp. 321-324.

543 C. trav. Liège, 14 septembre 2020, R.G. n° 2019/AL/133, disponible sur www.terralaboris.be.

544 Cour eur. D.H. (gde ch.), arrêt *Bărbulescu c. Roumanie*, 7 septembre 2017, req. n° 61496/08, commenté dans la *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, *R.D.T.I.*, 2017, n° 68-69, p. 134.

545 C. trav. Liège, 7 mai 2019, R.G. n° 2018/AL/128, *Chron. D.S.*, 2020, liv. 8-9, p. 359.

### *2. Gestion et usage de l'adresse professionnelle*

**143. Expédition à une adresse professionnelle d'une communication privée.** Dans une décision du 8 juin 2020, l'APD examinait la question de l'utilisation d'une adresse mail professionnelle pour réclamer des frais alimentaires dans le cadre d'un litige familial[546]. Le plaignant faisait grief à son ex-épouse de lui avoir adressé des communications liées à l'exécution d'un jugement prononcé par le tribunal de la famille sur une adresse mail professionnelle[547]. Ceci étant, l'APD va estimer que le RGPD s'applique aux parents et que l'ex-conjointe ne pouvait se fonder sur un consentement, ni sur un intérêt légitime pour utiliser l'adresse mail professionnelle de son ex-conjoint dans le cadre de l'exécution du jugement prononcé par le tribunal de la famille.

**144. Clôture de la messagerie professionnelle d'un administrateur.** Suite à une plainte déposée par un ancien administrateur d'une entreprise, l'APD a été amenée à examiner les règles à respecter au regard du RGPD concernant la clôture de la messagerie professionnelle de l'administrateur disposant de plusieurs adresses professionnelles comportant son nom[548]. Dans le cas d'espèce, l'entreprise avait conservé l'adresse et mis en place un système de redirection automatique vers une autre adresse. L'APD considère qu'il incombe à l'entreprise de bloquer la messagerie électronique des titulaires ayant cessé leurs fonctions au plus tard le jour de leur départ effectif et de privilégier l'insertion d'un message automatique de réponse qui pourra être mise en place pendant une période d'un mois, voire jusque trois mois dans le cas du contexte particulier de la fonction occupée par la personne concernée, et ce moyennant accord ou avertissement de la personne concernée. L'APD considère qu'ensuite, il convient de supprimer la messagerie électronique[549].

**145. Envoi d'un e-mail à des tiers avec adresse visible pour tous.** Dans le cadre d'une affaire tournant autour de l'envoi d'un mail par une société à l'ensemble de ses clients, envoyé par erreur en « copie » au lieu de l'être en « copie cachée », ce qui occasionna un partage des données de contact de l'ensemble de la liste, à l'ensemble des clients de la société, l'APD a déclaré que ce type d'erreur violait certes le RGPD (violation du principe de responsabilité, du principe de finalité et absence de base de licéité), mais n'était pas de nature, en l'espèce, à justifier l'imposition d'une amende administrative (simple réprimande)[550].

546 APD, 8 juin 2020, décision n° 29/2020.

547 Il est à noter que l'APD n'examine pas spécifiquement si le traitement litigieux entre effectivement dans le champ d'application du RGPD. Or, s'agissant d'un litige d'ordre familial et d'un traitement lié à des communications entre les parents d'un enfant commun à propos d'un décompte de frais, il ne nous semble pas évident que ce traitement ne puisse pas relever de l'exception prévue à l'article 2, 1, c), du RGPD qui prévoit que ce règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique dans le cadre d'une activité strictement personnelle ou domestique.

548 APD, 29 septembre 2020, décision n° 64/2020.

549 Sans entrer dans le détail de ce qu'il en est de la récupération éventuelle de courriers pertinents pour le fonctionnement de l'entreprise, l'Autorité renvoie à la Recommandation CM/REC (2015) sur le traitement des données à caractère personnel dans le cadre de l'emploi du Comité des ministres du Conseil de l'Europe qui précise que, « si le contenu de la messagerie devait être récupéré pour la bonne marche de l'organisation, l'employeur devrait prendre des mesures appropriées afin de récupérer son contenu avant le départ de l'employé et, si possible, en sa présence ». La décision est ambiguë concernant l'objet de la suppression. On comprend que le litige porte sur la suppression de l'adresse électronique.

550 APD, 2 avril 2019, décision n° 02/2019.

### *3. Contrôle et prise de connaissance de fichiers*

**146. Contrôles de fichiers.** Dans un arrêt *Libert* qui concernait la prise de connaissance de fichiers sur un support de l'employeur[551], la Cour européenne des droits de l'homme vérifie si l'ingérence consistant en une prise de connaissance de fichiers sur le disque dur d'un travailleur par un employeur assimilé à une autorité publique (en l'occurrence, la SNCF) est admissible. Sur la question de la proportionnalité, la Cour va estimer que les juridictions nationales ont pu considérer que l'accès aux fichiers par l'employeur pouvait dans ce cas intervenir hors de la présence du travailleur en application d'un règlement interne qui ne prévoyait de mesures spécifiques que lorsqu'il s'agissait d'accéder à des documents privés.

### *4. Enregistrement audio de conversations téléphoniques*

**147. Critère des attentes raisonnables.** Se référant à l'arrêt de la Cour de cassation du 9 septembre 2008[552], la Cour du travail de Mons a, dans un arrêt du 19 décembre 2019, considéré comme illégal l'enregistrement effectué par un responsable de ses conversations avec deux clientes d'une travailleuse qui avait été licenciée pour motif grave[553]. La Cour a en effet estimé que ces deux clientes ne pouvaient s'attendre à être enregistrées. Elle relève incidemment que la conversation avait en outre été orientée et détournée par rapport au sujet principal pour aborder les questions qui permettaient d'obtenir des informations sur les pratiques de la travailleuse concernée. Elle écarte des débats ces enregistrements audio.

C'est également sous l'angle du critère des attentes raisonnables que le tribunal du travail de Liège a, dans un jugement du 6 novembre 2020, écarté des débats un enregistrement audio effectué par une travailleuse postérieurement à son licenciement[554]. Cette travailleuse avait enregistré une conversation avec l'administratrice déléguée de son ancien employeur, en vue d'établir l'existence d'un accord sur le paiement d'heures supplémentaires discuté lors d'un entretien téléphonique. Le tribunal relève que l'administratrice ne pouvait s'attendre à être enregistrée au vu du contexte et de la teneur de l'entretien. Implicitement, le tribunal considère en outre le procédé disproportionné, relevant que la travailleuse n'avait plus rien à craindre puisque son contrat de travail avait déjà pris fin et aurait pu demander qu'un accord écrit soit rédigé. Selon le tribunal, elle ne se trouvait pas dans une situation nécessitant de recourir à ce type de pratique pour sauvegarder ses droits.

**148. Droit de se constituer une preuve.** En se fondant essentiellement sur les critères relatifs à l'admissibilité de la preuve qui découlent de l'application de la jurisprudence Antigone, le tribunal du travail de Liège, division Liège, a, dans un jugement du 27 novembre 2018, estimé que l'enregistrement d'une conversation téléphonique professionnelle à l'insu de l'un de ses interlocuteurs est irrégulier, mais proportionné au but recherché[555]. En l'occurrence il s'agissait de se réserver une preuve d'un comportement illégal par un moyen irrégulier, mais, à l'estime du tribunal, relativement peu attentatoire au respect de la vie privée. Cet enregistrement visait à établir qu'aucun

551 Cour eur. D.H., arrêt *Libert c. France*, 22 février 2018, req. n° 588/13.
552 Cass., 9 septembre 2008, R.G. n° P.08.0276.N.
553 C. trav. Mons, 19 décembre 2019, R.G. n° 2018/AM/376, *B.J.S.*, 2020/645, pp. 5-41.
554 T. trav. Liège, 6 novembre 2020, R.G. n° 18/3848/A, inédit.
555 T. trav. Liège, 27 novembre 2018, R.G. n° 17/4153/A, *B.J.S.*, 2019/621, pp. 4-25.

avenant n'avait été signé entre les parties alors que l'employeur produisait un document qui laissait entendre le contraire.

### *5. Contrôle des données de localisation*

**149. Cadre légal.** Les quelques décisions examinées pointent le fait qu'en l'absence de loi ou de CCT particulière, la légalité de l'utilisation de données issues de relevés de « *tracking* » d'un système de géolocalisation associé à un GPS dans le cadre du contrat de travail s'apprécie essentiellement au regard du droit au respect de la vie privée et de la législation relative à la protection des données à caractère personnel (les faits étaient toutefois antérieurs à l'entrée en application du RGPD).

**150. Information préalable.** Dans un jugement du 9 avril 2019, le tribunal du travail du Brabant wallon, division Wavre, estime que le fait d'avoir conservé les rapports du système de « *track and trace* » associés à l'utilisation du véhicule de la travailleuse constitue une conservation et un traitement de données. Il s'appuie sur un avis de l'ancienne Commission de la protection de la vie privée[556] et la jurisprudence pour constater que la surveillance au moyen d'un système de navigation GPS doit être conforme aux principes de transparence, proportionnalité et finalité résultant de l'application de la loi du 8 décembre 1992[557]. Il suffira au tribunal de constater que la travailleuse n'avait pas été informée du traitement de ses données de géolocalisation pour considérer que les preuves recueillies l'ont été de manière irrégulière. Dans le même sens, une décision de la Cour du travail d'Anvers, division Hasselt, estime qu'est obtenue en violation du droit à la vie privée du travailleur la preuve issue d'un système de géolocalisation activé sans que la travailleuse ait reçu une information spécifique préalable, le seul élément résultant des pièces du dossier étant que la travailleuse était informée du fait que le véhicule était équipé d'un tel système[558].

**151. Proportionnalité.** Dans l'arrêt précité[559], la Cour juge par ailleurs que la surveillance était disproportionnée en ce qu'elle incluait également des déplacements en dehors des heures de travail, que la travailleuse ne pouvait désactiver le système de *tracking* GPS et que la surveillance ne se limitait donc pas aux déplacements professionnels, qui auraient pu justifier un contrôle légitime.

**152. *Car policy*.** Dans un jugement du tribunal du travail de Liège, division Liège, du 4 mars 2019, le tribunal examine la légalité d'un contrôle des déplacements d'un travailleur grâce aux données GPS sous l'angle des principes de légalité et transparence, de finalités et de proportionnalité. Il relève l'existence d'une « *car policy* » mentionnant explicitement l'existence d'un système de géolocalisation et les finalités d'utilisation, permettant de conclure au respect desdits principes[560]. Le tribunal pointe encore que, s'agissant d'un véhicule dont l'usage était réservé à des

556 Il est fait référence à l'avis n° 12/2005 du 7 septembre 2005 relatif à la proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée.

557 T. trav. Brabant wallon, 9 avril 2019, R.G. n° 14/1137/A, *J.L.M.B.*, 2020/29, p. 1349, note K. Rosier.

558 C. trav. Anvers, 26 juin 2018, R.G. n° 2017/AH/133, *Limb. Rechtsl.*, 2019, liv. 2, p. 143.

559 *Idem*.

560 T. trav. Liège, 4 mars 2019, R.G. n° 18/245/A, disponible sur http://www.terralaboris.be.

déplacements professionnels et ayant été averti spécifiquement de la possibilité d'un contrôle, le travailleur pouvait s'attendre à ce qu'il soit vérifié si des déplacements privés étaient effectués avec ce véhicule.

### *6. Vidéosurveillance en milieu professionnel*

**153. Caméra cachée – Arrêt de la grande chambre de la Cour européenne des droits de l'homme.** La période analysée a été marquée par un arrêt de la Grande chambre de la Cour européenne des droits de l'homme se prononçant sur une mesure de vidéosurveillance cachée au regard de l'article 8 de la CEDH[561]. Dans cet arrêt *López Ribalda*, la Cour rappelle qu'un État n'a pas l'obligation de réglementer le recours à la vidéosurveillance dans le contexte d'un contrat de travail. Si une telle législation existe, cela n'empêche pas que les juridictions saisies d'un cas d'application de cette loi doivent s'assurer que la mise en place, par un employeur, de mesures de surveillance portant atteinte aux droits à la vie privée ou au secret des correspondances des travailleurs est proportionnée et s'accompagne de garanties adéquates et suffisantes contre les abus. Dans la lignée de l'arrêt *Bărbulescu*, la Cour dégage des critères qui doivent conduire à une appréciation globale de l'ensemble des circonstances, parmi lesquels un critère de transparence. La Cour décide que l'absence de respect d'une obligation d'information légale préalable n'implique pas nécessairement la violation de l'article 8, mais a pour conséquence que les autres critères qui permettent d'apprécier la proportionnalité de la mesure doivent être appliqués plus strictement.

**154. Caméra cachée – Champ d'application de la CCT n° 68.** À propos de l'exploitation d'images recueillies par une caméra non signalée, une décision du 4 février 2019 du tribunal du travail du Hainaut, division Charleroi, fait spécifiquement référence à cet arrêt[562]. En l'occurrence, un travailleur licencié contestait la régularité de l'utilisation d'images provenant d'une caméra installée par un tiers sur un stand publicitaire dans le contexte d'une foire d'expositions[563]. Le tribunal a estimé que, si la CCT n° 68 ne visait effectivement pas les images vidéo recueillies par des tiers, les principes de cette convention collective de travail doivent être appliqués, en particulier en ce qui concerne l'interdiction de recourir à une caméra cachée. Si l'employeur ne peut pas lui-même utiliser une caméra cachée, il ne doit pas être plus légitime de recourir à des images recueillies de manière secrète par le biais d'un tiers. Cette décision a fait l'objet d'un appel et la Cour du travail saisie a considéré que la CCT n° 68 et la loi du 21 mars 2007 n'étant pas applicables, c'est sous l'angle d'une violation du droit au respect de la vie privée consacrée par l'article 8 de la CEDH qu'il convenait de raisonner[564].

**155. CCT n° 68 – Information préalable.** Dans une décision du tribunal du travail de Liège, division Dinant, le tribunal admet la preuve résultant d'images de vidéosurveillance prises dans

561 Cour eur. D.H. (gde ch.), arrêt *López Ribalda et autres c. Espagne*, 17 octobre 2019, req. n$^{os}$ 874/13 et 8567/13. Pour un commentaire de cet arrêt, voy. K. Rosier, « Vidéosurveillance sur le lieu du travail : entre protection des données et droit au respect de la vie privée », *R.D.T.I.*, 2020/80, pp. 77 et s.

562 T. trav. Hainaut, 4 février 2019, R.G. n° 17/2.779/A, cité par X., « Caméras de vidéosurveillance et constatation de motif grave : légalité ? », disponible sur http://www.terralaboris.be.

563 Sur la question du champ d'application de la CCT n° 68, l'APD a logiquement considéré que la CCT n° 68 ne s'appliquait pas à l'usage d'une caméra installée dans un magasin à l'égard des clients de celui-ci (APD, 13 mai 2020, décision n° 23/2020).

564 C. trav. Mons, 26 mai 2020, R.G. n° 2019/AM/167, disponible sur www.terralaboris.be.

un entrepôt, sur le lieu du travail, après avoir constaté que le règlement de travail dont le travailleur avait bien reçu copie prévoyait des dispositions à cet égard[565].

### *7. Prise de connaissance de propos sur les réseaux sociaux*

**156. Propos tenus sur des réseaux sociaux – Caractère public.** Dans un arrêt de la Cour du travail de Mons du 27 avril 2018, celle-ci a rappelé que les informations publiées sur une page *Facebook* « publique » à laquelle tout internaute a accès, voire même celle dont l'accès est limité aux « amis » du titulaire du profil, mais également « aux amis de ses amis », perdent leur nature privée. La Cour poursuit en indiquant que « quant aux informations accessibles sur la page aux seuls "amis" du travailleur intéressé, elles seront considérées comme publiques lorsque le nombre d'"amis" du travailleur est important ou lorsque certains d'entre eux font partie du personnel de l'entreprise »[566]. En l'occurrence le travailleur se voyait reprocher d'avoir publié sur sa page Facebook des propos et caricatures dénigrantes et portant atteinte à l'honneur et l'autorité de l'employeur représenté par son directeur. La Cour relève que, parmi les amis *Facebook* de ce travailleur se trouvait bon nombre de collègues qui avaient accès à ces publications et les avaient commentées.

Dans le même sens, le tribunal du travail du Hainaut, division Charleroi, a considéré qu'une travailleuse ne peut se prévaloir d'une prise de connaissance irrégulière d'une information transmise par voie électronique qui ne lui était pas destinée personnellement, s'agissant de propos qu'elle a tenu sur son profil *Facebook*[567]. La travailleuse invoquait n'avoir pas eu l'intention d'assurer une publicité à ses propos, mais le tribunal a pointé qu'il n'était pas plausible qu'une utilisatrice âgée de 32 ans d'un réseau social utilisé par des millions de personnes dans le monde ait pu ignorer que les publications réalisées via son profil étaient accessibles à tous les internautes dont, potentiellement, son employeur. Il précise encore que, dès lors que la travailleuse n'ayant pas paramétré son compte afin que ses publications ne soient visibles que par un nombre (très) limité de personnes, ce qu'elle pouvait faire lors de la création de son compte et par la suite à tout moment, elle doit en accepter le caractère public.

Toujours dans le même ordre d'idées, mais cette fois au sujet d'un forum RH où des professionnels du secteur partageaient entre eux leurs conseils, qualifiés par la Cour de « propos relevant d'un débat d'intérêt public », la Cour européenne des droits de l'homme a rappelé encore une fois qu'un travailleur conserve son droit à la liberté d'expression et qu'il ne peut être licencié pour des propos tenus sur internet sans que soit réalisée « une mise en balance du droit à la liberté d'expression du requérant, dans le contexte de sa relation professionnelle, à l'aune du droit de son employeur à la protection de ses intérêts commerciaux ». La banque qui l'employait considérait en effet que ce type d'échange d'information portait atteinte à ses intérêts commerciaux, position que la Cour n'a pas suivie. Elle a considéré que les juridictions internes n'avaient pas tenu compte du droit à la liberté d'expression de l'employé puisque « l'issue du litige professionnel a été purement dictée par des considérations contractuelles entre la banque et le requérant »[568].

565 T. trav. Liège, 2 octobre 2020, R.G. n° 19/363/A, inédit.
566 C. trav. Mons, 27 avril 2018, R.G. n° 2017-AM-367, *Sem. soc. /Soc. Week.*, 2019/3.
567 T. trav. Hainaut, 1er octobre 2018, R.G. n° 17/1.039/A, disponible sur www.terralaboris.be.
568 Cour eur. D.H., arrêt *Herbai c. Hongrie*, 5 novembre 2019, req. n° 11608/15.

### *8. Sort des preuves irrégulières*

**157. Droit à un procès équitable – Éclairage de la Cour européenne des droits de l'homme.** Dans l'arrêt *López Ribalda*, la Cour se prononce sur la question de l'admissibilité des preuves. Elle rappelle que si l'article 6 de la CEDH garantit le droit à un procès équitable, cela n'empêche pas que des règles relatives à l'admissibilité des preuves relèvent du droit interne[569]. L'arrêt met en avant des critères pour vérifier si la preuve obtenue peut être utilisée sans violer le droit à un procès équitable. Ils renvoient à la possibilité de faire valoir devant les juridictions nationales les griefs tirés d'une violation des droits fondamentaux pour s'opposer à l'utilisation de la preuve et d'en contester l'authenticité. La Cour pointe également la prise en considération par les juridictions nationales du critère de qualité de la preuve[570].

**158. Jurisprudence Antigone – Preuves non écartées.** Parmi les décisions analysées, plusieurs concluent à l'existence d'une irrégularité de la preuve, mais estiment que, s'agissant de violations non sanctionnées de nullité, aucun critère de cette jurisprudence n'est rencontré qui justifierait que la preuve doive être écartée[571].

**159. Jurisprudence Antigone – Droit à un procès équitable – Déloyauté.** Dans une décision faisant application de la jurisprudence Antigone, le tribunal du travail de Liège, division Liège, écarte un enregistrement audio d'une conversation téléphonique au motif d'une atteinte aux droits de l'employeur un procès équitable, en se référant l'article 6 de la CEDH[572]. Pour parvenir à cette conclusion, il relève que l'enregistrement réalisé à l'insu d'une administratrice déléguée de l'employeur pourrait fausser le débat dans la mesure où la travailleuse qui le dépose avait choisi de s'adresser à une autre personne que son interlocutrice habituelle pour mener une discussion sur le paiement d'heures supplémentaires, alors que l'administratrice ne disposait pas des éléments pour mener une discussion sur ce point et a pu tenir des propos en vue d'apaiser la situation.

**160. Jurisprudence Antigone – Droit à un procès équitable – Proportionnalité.** La Cour du travail de Mons a considéré dans le cadre de l'appréciation de la recevabilité d'images vidéo obtenues en violation de l'article 8 de la CEDH que les critères de la jurisprudence Antigone doivent amener à une mise en balance du droit à la preuve de l'employeur et du respect des droits fondamentaux du travailleur. La Cour ajoute qu'il y a lieu de tenir compte des circonstances de la violation, de son objet et de son incidence sur le droit à un procès équitable. En l'espèce, la Cour n'écarte pas la preuve au motif que l'obtention des images était fortuite (caméra installée par un tiers dans une foire) et que l'employeur ne disposait pas d'autres moyens d'établir le comportement (soupçon de vol) du travailleur qui travaillait seul de nuit. La Cour relève également que le travailleur avait eu la possibilité de prendre connaissance des images avant son licenciement et la preuve a fait l'objet d'un débat judiciaire contradictoire[573].

569 Cour eur. D.H. (gde ch.), arrêt *López Ribalda et autres c. Espagne*, 17 octobre 2019, req. n$^{os}$ 874/13 et 8567/13.

570 Pour des décisions qui se réfèrent à cet arrêt concernant la prise en compte de preuves irrégulières, voy. T. trav. Hainaut, 4 février 2019, R.G. n° 17/2.779/A, citée par X., « Caméras de vidéosurveillance et constatation de motif grave : légalité ? », http://www.terralaboris.be/spip.php?article2773 et T. trav. Liège, 2 octobre 2020, R.G. n° 19/363/A, inédit.

571 C. trav. Gand, 8 juin 2018, *R.W.*, 2020-2021/4, pp. 145-146.

572 T. trav. Liège, 6 novembre 2020, R.G. n° 18/3848/A, inédit.

573 C. trav. Mons, 26 mai 2020, R.G. n° 2019/AM/167, disponible sur www.terralaboris.be.

Dans le même sens, la Cour du travail de Liège examine la question de la recevabilité à l'aune de l'article 6 de la CEDH, ainsi que la jurisprudence de la Cour constitutionnelle et la Cour de cassation. Elle épingle en particulier le critère de la proportionnalité et estime qu'il y a lieu de vérifier si le droit d'une partie de présenter à une juridiction des preuves recueillies de manière illégale ou déloyale peut l'emporter sur le droit de son adversaire au respect de ses droits fondamentaux parmi lesquels le droit au respect de sa vie privée. En l'espèce, elle relève le caractère disproportionné de l'atteinte causée au droit de la vie privée de la travailleuse, au regard des manquements qui lui sont concrètement reprochés, en l'occurrence d'avoir utilisé sa messagerie à des fins privées. La Cour relève que l'usage privé n'était pas proscrit, mais devait être limité et que les e-mails n'établissaient pas une utilisation particulièrement importante de la messagerie à des fins privées, alors que le contrôle a porté sur une période non limitée dans le temps qui incluait des e-mails privés et le contenu des e-mails, le tout sans respecter le prescrit de la CCT n° 81. Elle conclut au caractère disproportionné de l'atteinte aux droits du travailleur[574].

Après avoir constaté que des communications électroniques ont été obtenues sans le consentement du travailleur, la troisième chambre de la Cour du travail de Bruxelles estime que les preuves sont toutefois recevables nonobstant cette irrégularité dès lors que les critères de la jurisprudence Antigone ne conduisent pas à écarter les preuves. En particulier, la Cour conclut, au terme du test de proportionnalité, que l'atteinte portée à la vie privée de la travailleuse est moindre que les atteintes que le contrôle de ces e-mails a permis de mettre en évidence (communication de données confidentielles d'une société concurrente)[575].

**161. Jurisprudence Antigone – Non-application dans un litige civil.** Dans un arrêt du 22 février 2018, la quatrième chambre de la Cour du travail de Bruxelles se rallie à la position développée par la Cour du travail dans un arrêt largement commenté du 7 février 2013[576], qui considérait que cette jurisprudence ne s'applique pas dans le cadre d'un contrat de travail qui relève du domaine civil. Plus particulièrement la Cour considère que décider autrement reviendrait à faire primer le droit de la surveillance de l'employeur sur le droit au respect de la vie privée du travailleur, alors qu'à l'inverse du premier, il s'agit d'un droit fondamental[577].

## E. Traitements de données à caractère personnel et e-gouvernement

### *1. Utilisation des données personnelles des citoyens à des fins électorales*

**162. Données à caractère personnel des électeurs.** Durant la période étudiée au sein de la présente chronique, la Chambre contentieuse de l'APD a été amenée à statuer sur plusieurs plaintes déposées par des citoyens dont les données à caractère personnel avaient été réutilisées à des fins électorales[578].

574 C. trav. Liège, 7 mai 2019, R.G. n° 2018/AL/128, *Chron. D.S.*, 2020, liv. 8-9, p. 359.

575 C. trav. Bruxelles, 8 février 2019, *J.T.T.*, 2019/18, décision n° 1342, pp. 321-324.

576 C. trav. Bruxelles, 7 février 2013, R.G. n° 2012/AB/1115 ; *J.T.*, 2013, liv. 6516, note D. Mougenot ; *Ors.*, 2013, (Reflet B. Paternostre), liv. 4, p. 25 ; *Chron. D.S.*, 2013, liv. 2, p. 106, note O. Rijckaert.

577 C. trav. Bruxelles, 22 février 2018, R.G. n° 2015-AB-438, *Sem. soc. /Soc. Week.*, 2018/36 ; dans le même sens, voy. T. trav. Brabant wallon, 9 avril 2019, R.G. n° 14/1137/A, *J.L.M.B.*, 2020/29, p. 1349, note K. Rosier.

578 Certaines de ces décisions ont déjà rapidement été évoquées précédemment, voy. *supra*, § 81.

Dans les faits ayant abouti à la décision du 28 mai 2019[579], un bourgmestre avait utilisé à des fins électorales l'adresse e-mail de deux citoyens, initialement communiquée pour une finalité bien précise. Lors d'un contact par e-mail avec le bourgmestre au sujet d'une question urbanistique, l'architecte des plaignants avait mis ses clients en copie de l'e-mail. À la veille des élections communales, le bourgmestre reprend cet e-mail en utilisant la fonction « répondre à tous » pour envoyer de la propagande électorale aux plaignants. L'APD décide qu'en réutilisant l'adresse e-mail des plaignants à des fins électorales, le bourgmestre opère un détournement de finalité et viole les articles 5.1.b) et 6.4 du RGPD. L'APD insiste également sur le fait que le respect du RGPD est une obligation sérieuse à respecter, *a fortiori* pour un titulaire de mandat public, qui doit montrer l'exemple. La Chambre contentieuse en conclut une violation grave du RGPD et impose une réprimande, une amende administrative de 2.000 euros et la publication de sa décision, anonymisée, sur son site internet.

En novembre 2019, l'APD a eu à connaître d'un cas similaire[580] à l'occasion duquel un bourgmestre avait envoyé un courrier de propagande électorale à un citoyen de sa commune, au moyen d'un fichier de coordonnées croisé à la liste communale des électeurs. Le plaignant avait, un jour, accompagné son voisin à un rendez-vous avec le bourgmestre. Ce dernier a constitué une liste des citoyens de la commune l'ayant sollicité en sa qualité de bourgmestre et leur envoie, à l'approche des élections, un courrier de propagande électorale. À l'occasion de sa décision, l'APD prend soin de rappeler l'existence du principe de finalité consacré à l'article 5.1.b) du RGPD et le met en parallèle avec une note « Élections » qu'elle a rédigée dans le début des années 2000. Cette note prévoit expressément qu'il n'est pas permis de réutiliser des données à caractère personnel obtenues dans le cadre d'un mandat échevinal pour faire de la propagande électorale, sous peine de réaliser un traitement incompatible avec les finalités pour lesquelles ces données ont été collectées. Estimant que le fait pour un bourgmestre d'avoir croisé un nombre conséquent de données personnelles de citoyens l'ayant consulté entre 2012 et 2018 avec la liste des électeurs pour leur adresser un courrier ne rentrait pas dans le cadre d'une exception prévue à l'article 6.4 du RGPD, la Chambre contentieuse conclut à une violation du RGPD (articles 5.1.b) et 6.4). L'APD insiste également sur la qualité de mandataire public du bourgmestre pour justifier le caractère grave de ses manquements et pour finalement prononcer une réprimande à son encontre, le condamner à une sanction administrative de 5.000 euros et ordonner la publication de sa décision sur son site internet.

Une plainte similaire à celles au sujet desquelles l'APD a été saisie dans les deux affaires précitées a été déposée par un plaignant ayant reçu un courrier de propagande électorale d'un échevin, candidat aux élections, exerçant en qualité de vétérinaire dans la commune[581]. Le plaignant invoque devant la Chambre contentieuse que le courrier a été adressé à son ancienne adresse, là où il habitait du temps où il était client du cabinet vétérinaire de l'échevin. L'obtention de son adresse postale ne peut donc être issue que d'une réutilisation, par le candidat aux élections, de son fichier client lié à son activité de vétérinaire. Tout comme dans la décision n° 10/2019, l'APD rappelle qu'elle n'est pas compétente pour se prononcer sur une éventuelle violation du règle-

579 APD, 28 mai 2019, décision n° 4/2019.
580 APD, 25 novembre 2019, décision n° 10/2019.
581 APD, 25 novembre 2019, décision n° 11/2019.

ment d'ordre intérieur du Conseil communal de la commune en question. S'agissant du fond, celle-ci renvoie, tout comme dans la décision 10/2019, à sa note « Élections » et renvoie également expressément à sa décision 04/2019 résumée ci-dessus. L'APD estime qu'en utilisant un fichier professionnel constitué au départ de données à caractère personnel de clients le consultant en qualité de vétérinaire pour envoyer des courriers électoraux, le candidat a traité les données de manière incompatible avec la finalité initiale de la collecte (fût-elle licite), en méconnaissance des articles 5.1.b) et 6.4 du RGPD. Comme dans ses précédentes décisions, elle estime que la qualité d'échevin aurait dû s'accompagner d'un « comportement exemplaire » et, outre une réprimande et la publication de la décision, ordonne la condamnation de celui-ci à une amende administrative de 5.000 EUR.

Une plainte a été déposée dans une autre affaire, dans laquelle une citoyenne d'une commune avait réceptionné un courrier de propagande électorale de l'administratrice d'une ASBL à laquelle la citoyenne avait fait appel pour recevoir des soins infirmiers[582]. L'APD sanctionne l'ASBL pour manquement à son devoir d'accès et lui ordonne de faire droit à la demande d'effacement de la plaignante, compte tenu notamment du caractère sensible (données de santé) des données traitées. L'ABSL écope également d'une amende administrative pour violations du RGPD.

Dans le cadre d'un autre litige, tranché par l'APD le 8 juin 2020[583], une plainte avait été déposée par une commune à l'encontre du défendeur, tête de liste d'un parti politique, pour utilisation d'une liste du personnel de la commune (agents communaux) aux fins de leur envoyer un courrier de propagande électorale. 68 personnes étaient concernées, dont la directrice générale de la commune et le délégué à la protection des données. Cette décision est intéressante en ce qu'elle rappelle que les personnes morales, les associations et les institutions peuvent, si elles souhaitent dénoncer une infraction au RGPD, saisir l'APD, au même titre que les personnes physiques. Pour le surplus, la Chambre contentieuse considère qu'il est établi que les données figurant sur la liste du personnel ont été traitées pour d'autres fins (propagande électorale) que celles pour lesquelles elles ont été collectées et conclut à une violation des articles 5.1.a), 5.1.b) et 6.1 du RGPD, caractérisée également par la qualité du défendeur, tête de liste aux élections. Celui-ci se voit infliger une amende de 5.000 euros.

En date du 28 juillet 2020[584], l'APD a traité la plainte d'une habitante d'une commune, qui avait réceptionné un courrier postal de propagande électorale destiné aux « nouveaux habitants » de la commune. La plaignante estimait que le parti n'avait pu avoir connaissance de son arrivée dans la commune qu'en ayant recours à d'autres données que la simple liste des électeurs. Au terme d'une enquête, l'APD constate que le parti a comparé la liste des électeurs de 2012 à celle des électeurs de 2018 et qu'il s'agit d'une violation du principe de limitation des finalités prévu par le RGPD. Sur la base du test de finalité, du test de nécessité et du test de pondération, la Chambre contentieuse constate que le traitement est illicite en ce que le responsable de traitement a modifié et structuré des données personnelles pour en extraire une « liste des nouveaux habitants ». Le défendeur (tête de liste du parti) est rappelé à l'ordre et se voit infliger une amende de 3.000 euros.

582 APD, 17 décembre 2019, décision n° 13/2019.
583 APD, 8 juin 2020, décision n° 30/2020.
584 APD, 28 juillet 2020, décision n° 39/2020.

Enfin, à l'occasion d'une décision du 1er septembre 2020[585], l'APD s'est à nouveau penchée sur l'utilisation, par un bourgmestre, de l'adresse e-mail d'un citoyen, obtenue à l'occasion de l'envoi d'un e-mail à son secrétariat par le citoyen en question quelques années plus tôt, pour dénoncer un problème de propreté publique. La Chambre contentieuse estime que l'adresse e-mail du citoyen devait être traitée uniquement pour répondre à sa question, et non pour lui envoyer du courrier électoral. La chambre conclut, sur les mêmes bases que dans les décisions précédentes, à plusieurs violations du RGPD et impose une amende de 5.000 euros au bourgmestre concerné.

### *2. Utilisation de la carte d'identité électronique (et des données personnelles y contenues) comme carte de fidélité*

**163. L'e-ID comme carte de fidélité.** L'APD a été amenée à se prononcer sur le bien-fondé d'une plainte déposée par un citoyen à l'encontre d'un commerçant qui imposait l'utilisation de la carte d'identité électronique comme carte de fidélité[586]. L'APD se réfère aux dispositions du RGPD et également à la loi belge du 19 juillet 1991[587] relative notamment aux cartes d'identité qui prévoit, depuis le 23 décembre 2018, que la carte d'identité électronique ne peut être lue ou utilisée qu'avec le consentement de son titulaire et, si elle l'est dans le cadre d'un avantage ou un service proposé au citoyen, seulement si une alternative est proposée à ce dernier. La Chambre contentieuse estime, sur la base de cette disposition ainsi que du RGPD, que trois infractions doivent être constatées dans le chef du commerçant : une violation du principe de minimisation des données (i), une atteinte au principe de légalité du traitement (ii) et une violation du principe de transparence (iii). Pour ces raisons, elle ordonne au commerçant de se mettre en conformité par rapport aux infractions constatées, lui inflige une amende administrative de 10.000 euros et ordonne la publication de sa décision sur son propre site internet.

La décision a fait l'objet d'un recours devant la Cour des marchés, qui l'a invalidée[588]. Dans sa décision, la Cour considère notamment que l'APD n'a pas prouvé suffisamment qu'un traitement de ces données avait eu lieu (vu le refus du plaignant de consentir à ce traitement), qu'elle base en partie son analyse sur une version de l'article 6 de la loi du 19 juillet 1991 qui n'était pas applicable au moment des faits et qu'elle n'avait pas suffisamment motivé le montant de l'amende. La Cour des marchés ne valide donc pas pour autant l'existence de telles pratiques commerciales[589].

### *3. Atteinte au droit d'accès aux données par une autorité publique*

**164. Droit d'accès de la personne concernée.** L'APD a été amenée à se prononcer sur l'absence de suite donnée à l'exercice du droit d'accès par un citoyen désirant connaître les motifs du retrait de sa fonction[590]. Elle se réfère aux dispositions du RGPD et constate que l'autorité publique – ici

585 APD, 1er septembre 2020, décision n° 53/2020.

586 APD, 17 septembre 2019, décision n° 6/2019.

587 Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour.

588 Bruxelles (Cour des marchés), 19 février 2020, R.G. n° 2019/AR/1600, disponible sur le site de l'APD.

589 La Cour a néanmoins considéré que l'APD avait été trop catégorique concernant le caractère nécessairement « non libre » du consentement, vu le caractère peu important de l'avantage auquel il n'aurait pas droit en refusant d'autoriser l'exploitation des données contenues dans la carte d'identité.

590 APD, 9 juillet 2019, décision n° 5/2019.

le SPF Santé publique – n'a pas respecté le droit d'accès du plaignant, lequel exerçait son droit dans l'objectif d'avoir connaissance des motifs justifiant le retrait de sa fonction de membre d'une commission médicale provinciale. La Chambre contentieuse constate que la demande d'accès du plaignant est restée sans réponse, et ce malgré une première décision de l'Autorité qui ordonnait au responsable du traitement de respecter la demande de la personne concernée. Forte de ce constat, la Chambre contentieuse estime que l'autorité publique s'est rendue coupable de deux violations du RGPD : une violation du droit d'accès reconnu au plaignant par l'article 15 du RGPD (i), ainsi qu'un non-respect de l'obligation d'informer la personne concernée des suites réservées à la demande de la personne concernée imposée par les articles 12.3 et 12.4 du règlement (ii). La Chambre contentieuse souligne en outre « l'extrême négligence » dont a fait preuve le responsable du traitement dans la gestion de la demande du plaignant. Pour ces raisons, elle réprimande le SPF Santé publique et ordonne la publication de sa décision sur le site internet de l'Autorité. Cette décision a été annulée par la Cour des marchés pour défaut de motivation et excès de pouvoir[591].

### *4. Collecte de données à caractère personnel de locataires au moyen d'un formulaire fiscal*

**165. Formulaire communal et données des locataires.** L'APD a été amenée à se prononcer sur la validité d'un formulaire par lequel une commune demande aux propriétaires de collecter certaines données à caractère personnel de leurs locataires[592]. L'Autorité constate que le formulaire utilisé par la commune a pour but de déterminer si les locataires entrent dans les conditions pour bénéficier d'une réduction d'impôt. Ainsi, outre les données d'identification (noms, prénoms…), le propriétaire doit collecter les informations relatives au statut des locataires (étudiant ou non) ainsi qu'au montant de l'éventuelle bourse d'études dont ils bénéficient. Enfin, le formulaire prévoit également la collecte du numéro de téléphone d'un proche du locataire au titre de « numéro d'urgence ». L'APD estime que le traitement ainsi mis en place enfreint trois principes applicables au traitement de données à caractère personnel : une violation du principe de transparence reconnu par l'article 5.1.a) du RGPD, car la commune n'informe pas les locataires de l'existence du traitement et de ses finalités (i), une violation du principe de finalité reconnu par l'article 5.1.b), car la donnée « numéro d'urgence » était collectée à des fins de sécurité publique et non à des fins fiscales (ii), et une violation du principe de minimisation des données reconnu par l'article 5.1.c) du RGPD, car la donnée « numéro d'urgence » n'est pas utile à la poursuite de la finalité fiscale. Pour ces raisons, et parce qu'il s'agit de violations sérieuses touchant aux principes fondamentaux mis en place par le RGPD, la Chambre contentieuse ordonne le gel du traitement jusqu'à sa mise en conformité avec ces principes.

### *5. Utilisation illégale des bases de données fédérales*

**166. Consultation du Registre national.** L'autorité de protection des données a été amenée à se prononcer sur la responsabilité d'une commune à la suite de la consultation irrégulière du Registre national par un membre de son personnel[593]. L'APD rappelle que la commune, en tant que responsable du traitement, est responsable du respect des obligations issues du RGPD en

591 Bruxelles (Cour des marchés), 23 octobre 2020, R.G. n° 2019/AR/1234, disponible sur le site de l'APD.
592 APD, 15 avril 2020, décision n° 15/2020.
593 APD, 29 avril 2020, décision n° 19/2020.

application du principe *d'accountability* reconnu par les articles 5.2 et 24 du RGPD. Parmi ces obligations, l'Autorité souligne tout particulièrement l'obligation de sécurité prévue par l'article 32 du RGPD qui précise le principe d'intégrité et de confidentialité reconnu par l'article 5.1.f) du RGPD. En application de ce principe, ainsi que de l'article 17 de la loi belge encadrant le Registre national, la commune est tenue de mettre en place un contrôle des accès au Registre national permettant de déterminer l'identité de tout agent qui accède au Registre, ainsi que la finalité pour laquelle il le fait. L'APD constate cependant qu'au moment de son inspection, tel n'était pas encore le cas. Partant, la commune se rend coupable d'une violation grave des principes d'*accountability* et d'intégrité des données. Bien que la commune démontre qu'elle a, depuis lors, adopté les mesures de sécurité nécessaires lui permettant, à terme, d'être en conformité avec le RGPD et le droit national, l'APD décide toutefois de la réprimander et ordonne la publication de la décision sur son site internet.

Dans le même sens, la consultation du Registre national par un organisme d'intérêt public, dans le cadre d'une instruction concernant une infraction de dépôt d'ordure clandestin, pour identifier les liens parentaux précis entre les différentes personnes vivant à l'endroit du dépôt clandestin a été considérée par l'APD comme un traitement non nécessaire à l'identification des contrevenants, violant donc le principe de minimisation des données[594]. À cette occasion l'APD rappelle encore une fois que l'accès à une base de données publique ne peut être utilisé que dans les cas où cela est strictement nécessaire à la mission pour laquelle l'accès à cette base de données est prévu.

**167. Accès à la Banque-Carrefour des véhicules (BCV).** L'autorité de protection des données a également été amenée à se prononcer sur l'utilisation des données de la Banque-Carrefour des véhicules (BCV) à des fins de marketing direct[595]. L'Autorité constate qu'une société commerciale (Informex) – qui est légalement associée à la gestion de la BCV – accède aux données de la BCV dans le but de les fournir à des sociétés d'assurances, qui les utilisent ensuite pour proposer des primes d'assurance personnalisées à leurs futurs clients. Le traitement ainsi réalisé par les assureurs se base sur le consentement du client, lequel accepte d'introduire son numéro de plaque d'immatriculation dans un formulaire en ligne. Une fois le numéro de plaque en sa possession, l'assureur peut lier l'identité du client à l'ensemble des informations relatives à son véhicule. L'APD constate que si Informex est légalement habilitée à accéder aux données de la BCV, cet accès est limité à la poursuite des finalités d'intérêt public qui sont reprises à l'article 4,4° de l'Arrêté royal du 8 juillet 2013. L'APD constate également que l'article 25 du même Arrêté royal interdit formellement l'utilisation des données à des fins de marketing direct. Or, en se référant à la définition qu'elle donne de cette pratique dans sa Recommandation 1/2020, elle considère que la pratique d'Informex est constitutive de marketing direct et est donc illégale. Par conséquent, l'APD considère que le traitement des données par Informex enfreint tant le principe de finalité reconnu par l'article 5.1.b) du RGPD, que le principe de licéité reconnu par l'article 6.1 du RGPD en ce qu'il poursuit une finalité interdite par le droit belge. L'APD ordonne au SPF Mobilité – responsable de la BCV – de mettre ce traitement de données en conformité avec la législation. Informex a interjeté appel de cette décision auprès de la Cour des marchés. La Cour a toutefois déclaré l'appel

[594] APD, 8 septembre 2020, décision n° 61/2020.
[595] APD, 23 juin 2020, décision n° 34/2020.

irrecevable, au motif qu'Informex n'était pas partie à la décision de l'Autorité de protection des données, puisque le défendeur était le SPF Mobilité (responsable de la BCV), et non Informex[596].

**168. Données issues du registre de la DIV.** Par un arrêt du 8 novembre 2018[597], la Cour constitutionnelle a tranché la question de savoir si, entre le 26 juin 2003 (date de l'entrée en vigueur de l'article 36*bis* de la loi du 8 décembre 1992) et le 24 mai 2018 (veille de l'entrée en vigueur du RGPD ayant abrogé la loi du 8 décembre 1992), les services de police pouvaient accéder aux données à caractère personnel des automobilistes enregistrées à la DIV, sans demander préalablement l'autorisation du Comité sectoriel Autorité fédérale. La Cour a jugé qu'un tel accès sans autorisation n'était possible que pendant une période limitée et a annulé l'article 3 de la loi du 14 juin 2017, soit la rétroactivité de la dispense d'autorisation du Comité sectoriel (et non la dispense elle-même)[598].

Plus récemment, l'APD a sanctionné une société spécialisée en stationnement de rue, qui avait accédé aux données disponibles à la DIV dès le lendemain du jour où le véhicule de la plaignante avait été contrôlé, et, à cette occasion, traité des données à caractère personnel (nom, prénom et adresse) de la plaignante sans nécessité. En effet, au moment du traitement, la plaignante avait encore l'occasion de s'acquitter de la redevance et le traitement de ces données (nécessaire par exemple pour envoyer un rappel de paiement) n'est pas conforme au principe de minimisation des données. La société (de même que l'étude de l'huissier de justice chargée de la récupération de la créance pour d'autres manquements) a été condamnée par l'APD[599].

596 Bruxelles (Cour des marchés), 28 octobre 2020, R.G. n° 2020/AR/1014, disponible sur le site de l'APD.

597 C.C., 8 novembre 2018, *R.D.T.I.*, 2018/4, p. 73.

598 Pour plus d'informations à ce sujet, voy. E. Degrave, « Protection des données et comités sectoriels : avant et après le RGPD », *R.D.T.I.*, 2018/4, pp. 91-97.

599 APD, 23 décembre 2020, décision n° 81/2020.