TITRE 20
La protection des données dans le secteur de la « police » et de la « justice »

Catherine FORGET[1]

Introduction

1. L'Union européenne a un parcours législatif marqué entre le besoin de faciliter les flux de données à des fins de sécurité nationale et la nécessité d'assurer le droit à la protection des données dans un domaine relevant initialement des prérogatives de la puissance publique. En dépit de ces difficultés, une première décision cadre fut adoptée, la décision-cadre 2008/977[2]. Celle-ci avait toutefois une portée limitée en raison de la limitation du champ d'application aux flux transfrontières de données sans être applicables aux traitements internes.

2. Récemment, dans le contexte de la lutte contre le terrorisme et la grande criminalité, parallèlement à l'adoption du règlement général sur la protection des données (ci-après RGPD)[3], l'Union européenne s'est donc dotée de la directive 2016/680/UE[4] (ci-après directive 2016/680/

[1] Avocate au barreau de Bruxelles (DWL-LAW) et chercheuse au CRIDS (Université de Namur).

[2] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.*, L 350/60 du 30 décembre 2008, pp. 60-71 (ci-après décision-cadre 2008/977/JAI).

[3] 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) (Texte présentant de l'intérêt pour l'EEE), *O.J.*, L 119 du 4 mai 2016, p. 1.

[4] Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à

UE) visant à réglementer la protection des données dans le secteur de la « police » et de la « justice ». Cette directive marque un tournant puisque, de manière inédite, elle encadre les traitements de données à caractère personnel des autorités compétentes, que ce traitement ait lieu sur le territoire interne des États membres ou au-delà. Ce faisant, la directive 2016/680/UE fixe une base commune de protection des données afin de faciliter l'échange d'informations entre les autorités répressives[5] et en ce sens, participe à la concrétisation de « l'espace de liberté, de sécurité et de justice ». Elle présente une certaine flexibilité, tant au niveau de la forme juridique choisie, à savoir, une directive plutôt qu'un règlement, qu'au niveau du fond, cherchant à ménager un certain équilibre entre le droit à la protection des données et les intérêts liés à la sécurité au sens large.

3. Comme nous l'analyserons dans le cadre de cette contribution, le régime de la directive 2016/680/UE est calqué sur celui du RGPD tout en présentant certaines singularités, notamment concernant les principes de licéité, de finalité et d'exactitude. Elle impose par ailleurs une catégorisation des données, encadre le traitement des catégories particulières de données. En outre, les droits des personnes concernées sont fortement tempérés en raison du contexte répressif ou judiciaire régulé dans lequel des règles particulières relatives au profilage sont également prévues. Par ailleurs, les États membres sont tenus d'instituer une autorité de contrôle indépendante chargée de vérifier le respect des règles édictées par la directive 2016/680/UE. Enfin, elle encadre les flux transfrontières des données dans le cadre des finalités visées par la directive.

4. Sur nombre de points, les notions et principes du RGPD sont donc repris dans la directive 2016/680/UE. Tel est le cas par exemple pour les concepts de responsable du traitement ou de sous-traitant. Aussi, c'est sans prétention d'exhaustivité que nous nous proposons d'examiner les grandes lignes de la directive en mettant en exergue ses spécificités par rapport au RGDP ainsi que certains points susceptibles de mener à des divergences d'interprétation ou à des difficultés, compte tenu notamment des recommandations du Contrôleur européen de la protection des données (ci-après CEPD) et du Groupe 29.

---

la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *O.J.*, L 119 du 4 mai 2016, pp. 89-131 (ci-après directive 2016/680). Pour un premier commentaire voy. P. De Hert et V. Papakonstantinou, *New Journal of European Criminal Law*, vol. 7, Issue 1, 2016, pp. 7-19.

[5] Communication de la Commission au Parlement européen, au conseil européen et au conseil, Quatrième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, Bruxelles, le 25 janvier 2017, COM 52017, 41 final.

CHAPITRE 1. Contexte historique

SECTION 1. – Les flux transfrontières de données en matière pénale

5. Le programme de La Haye, lancé pour une période de cinq ans par le Conseil européen de 2004, marque la volonté d'encadrer et de favoriser les flux transfrontières de données en matière pénale[6]. Ce programme prône en effet un échange d'informations selon le principe de « disponibilité », principe selon lequel les informations nécessaires dans le cadre de la lutte contre la criminalité doivent pouvoir traverser, sans entrave, les frontières intérieures de l'Union européenne (ci-après « UE ») et ainsi, être échangées aussi rapidement et aussi facilement que possible entre les services répressifs des États membres[7]. Dans la foulée, une décision-cadre visant à permettre la simplification de l'échange d'informations et de renseignements au sein de l'Union fut adoptée par l'UE en 2006[8] rappelant que l'accès rapide à des informations et à des renseignements précis et actualisés est essentiel pour permettre aux services répressifs de dépister et de prévenir la criminalité et d'enquêter sur elles, notamment dans un espace au sein duquel les contrôles aux frontières intérieures ont été supprimés[9].

6. Parallèlement, différents États membres, à savoir, l'Allemagne, la France, l'Espagne, les pays du Benelux et l'Autriche, ont adopté le Traité de Prüm afin d'approfondir la coopération en matière de lutte contre le terrorisme, la criminalité transfrontalière et la migration illégale[10]. En réponse à l'intérêt exprimé par plusieurs États membres d'adhérer à cet accord, l'Allemagne a proposé, au cours de sa présidence du Conseil de 2007, de le transformer en instrument de l'UE lequel fut formalisé partiel-

---

[6] Programme de La Haye du Conseil, *J.O.U.E.*, C 53 du 3 mars 2005.

[7] Point 2.1. du programme de La Haye. À ce propos, voy. Avis CEPD sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (COM (2005) 490 final), *J.O.U.E.*, C 116 du 17 mai 2006.

[8] Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, *J.O.C.E.*, L 386 du 29 décembre 2006, p. 89 (ci-après décision-cadre 2006/960/JAI).

[9] Considérant n° 4 de la décision-cadre 2006/960/JAI.

[10] Traité de Prüm du 27 mai *2005* entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière (ci-après Traité de Prüm).

lement par la décision de Prüm de 2008[11]. Celle-ci énonce les règles applicables à l'échange transfrontalier de profils ADN, d'empreintes digitales, de données relatives à l'immatriculation des véhicules et d'informations relatives aux personnes suspectées de planifier des attentats terroristes[12].

7. Récemment, dans le cadre de la coopération policière et judiciaire, de l'asile et de la migration, une proposition de règlement visant à permettre l'interopérabilité entre les systèmes d'information de l'UE a été déposée[13]. En effet, en dépit de l'augmentation des bases de données, les systèmes d'informations de l'UE restent cloisonnés de sorte que l'accès à l'information deviendrait plus complexe entraînant le risque « de laisser passer des informations à travers les mailles du filet et de permettre à des terroristes et des criminels d'échapper aux contrôles » par exemple, lorsqu'ils sont enregistrés sous des pseudonymes différents[14]. Dès lors, l'interopérabilité des systèmes d'information[15] vise à contribuer de manière appréciable à l'élimination des angles morts existants en permettant aux autorités compétentes de procéder au recoupement simultané des différents systèmes d'information tout en disposant d'un accès simplifié[16]. Notons toutefois qu'en mixant des finalités « répressives » et de « gestion des frontières », cette proposition laisse transparaître une tendance à la « crimmigra-

[11] Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, *J.O.*, L 210 du 6 août 2008, pp. 1-11 (ci-après Décision 2008/615/JAI).

[12] Art. 1 de la décision 2008/615/JAI.

[13] Proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité entre les systèmes d'information de l'UE (frontières et visas) et modifiant la décision 2004/512/CE du Conseil, le règlement (CE) 767/2008, la décision 2008/633/JAI du Conseil, le règlement (UE) 2016/399 et le règlement (UE) 2017/2226 et Proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité entre les systèmes d'information de l'UE (coopération policière et judiciaire, asile et migration), COM(2017) 793 final, 2017/0351 (COD), 12 décembre 2017.

[14] Commission européenne, Communiqué de presse, Union de la sécurité : la Commission comble les lacunes en matière d'information afin de mieux protéger les citoyens de l'Union, Strasbourg, le 12 décembre 2017.

[15] L'interopérabilité n'est pas une idée neuve mais a déjà fait l'objet d'une communication de la Commission en 2005. À ce propos, voy. P. De Hert et S. Gutwirth, « Interoperability of Police Databases within the EU : An Accountable Political Choice ? », *International Review of Law Computers and Technology*, vol. 20, n° 1-2, 2006, pp. 21-35.

[16] Les bases de données visées sont les systèmes d'information centralisés : le système d'information Schengen (SIS), le système Eurodac, le système d'information sur les visas (VIS), système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS) et le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (système ECRIS-TCN). Outre ces systèmes d'information, gérés de manière centrale au niveau de l'Union, le champ d'application de la présente proposition comprend également la base de données d'Interpol et Europol.

tion »[17], déjà critiquée à de nombreuses reprises par le passé dans le cadre des discussions relatives au VIS, SIS et EURODAC.

SECTION 2. – Les instruments de protection des données

Avant l'entrée en vigueur du Traité de Lisbonne, la législation relative à la protection des données était divisée entre le « premier pilier » (marché intérieur), le « deuxième pilier » (politique étrangère et de sécurité commune) et le « troisième pilier » (coopération policière et judiciaire)[18]. Dans le premier pilier par exemple, la protection des données était encadrée par la directive 95/46/CE[19]. Cette directive n'a pas vocation à encadrer la protection des données dans le domaine pénal de sorte que les règles de protection des données restaient de la compétence des États membres.

8. Plus tardivement et peu après les attentats terroristes de Londres et de Madrid en 2004 et 2005, l'Union européenne s'est dotée de la décision-cadre 2008/977[20], applicable dans le troisième pilier à savoir, la coopération policière et judiciaire en matière pénale. Son objectif est d'améliorer la coopération entre services répressifs, en particulier lorsqu'il s'agit de prévenir et de combattre le terrorisme, en respectant strictement les principes essentiels en matière de protection des données. Elle fut néanmoins fortement critiquée en raison du déséquilibre patent en faveur des impératifs de sécurité publique et au détriment de la protection des droits fondamentaux[21]. De plus, son impact fut relativement limité, la décision-cadre

[17] Le concept de « crimmigration » a été développé par des chercheurs établissant un lien entre l'immigration et la criminalité. Voy. J. Parkin, « The Criminalisation of Migration in Europe : A State-of-the-Art of the Academic Literature and Research », *CEPS Liberty and Security in Europe*, n° 61, 2013.

[18] Pour une analyse voy. F. Dumorter et Y. Poullet, « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne », *Défis du droit à la protection à la vie privée*, vol. 31, 2008.

[19] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.*, L 281 du 23 novembre 1995, pp. 0031-0050.

[20] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.*, L350/60 du 30 décembre 2008, pp. 60-71 (ci-après décision-cadre 2008/977/JAI).

[21] CEPD, avis du 27 avril 2007, *J.O.U.E.*, C 139/1 du 23 juin 2007 ; F. Dumortier, C. Gayrel, J. Jouret, D. Moreau et Y. Poullet, « La protection des données dans l'Espace

excluant de son champ d'application les traitements de données réalisés sur le territoire national des États membres[22].

9. Parallèlement, le droit à la protection des données a évolué au fil de la jurisprudence de la Cour de justice de l'Union européenne (ci-après, « C.J.U.E. ») laquelle se réfère abondamment à la Convention européenne des droits de l'homme (ci-après, « Convention ») mais aussi à la jurisprudence de la Cour européenne des droits de l'homme (ci-après, « Cour eur. D.H. »)[23]. Elle considère en effet devoir s'inspirer « des traditions constitutionnelles communes aux États membres ainsi que des indications fournies par les instruments internationaux concernant la protection des droits de l'homme auxquels les États membres ont coopéré ou adhéré »[24] en faisant expressément ou implicitement référence à la Convention[25].

10. De son côté, le Conseil de l'Europe a adopté des conventions ou des recommandations relatives à la protection des données, constituant des bonnes pratiques pour les États membres. En effet, à la différence de l'UE tiraillée entre le besoin d'assurer les flux transfrontières dans le cadre de la coopération policière et judiciaire tout en garantissant la protection des données, le Conseil de l'Europe s'est donné pour objectif unique de favoriser un espace démocratique et juridique commun organisé autour de la Convention en ce compris, le droit au respect de la vie privée. En ce sens, la Convention 108, seul instrument contraignant en matière de

européen de liberté, de sécurité et de justice », *J.D.E.*, 2010/2, n° 166, pp. 33 et s.

[22] Cette ambiguïté ne manqua pas d'être relevée par le CEPD soulignant qu'il peut s'avérer délicat de déterminer à l'avance si une information est susceptible de faire l'objet d'un flux transfrontière entre les États membres. CEPD, Avis du 19 décembre 2005 sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, *J.O.*, C47 du 25 février 2006.

[23] S. Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E. », in *Protection des droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2015, p. 225. Parallèlement à la mise en place d'un corps de règles relatifs à la protection des données dans le domaine de la coopération judiciaire et policière, la Cour de Strasbourg a, elle aussi, développé une jurisprudence riche et innovante concernant des traitements policiers, judiciaires ou de sûreté nationale (F. Dumortier, C. Gayrel, J. Jouret, D. Moreau et Y. Poullet, « La protection des données dans l'Espace européen de liberté, de sécurité et de justice », *op. cit.*, p. 34). Elle fut saisie de litige mettant directement ou indirectement en cause le droit de l'Union rappelant que « les parties contractantes sont responsables au titre de l'article 1er de la Convention de tous les actes et omissions de leurs organes, qu'ils découlent du droit interne ou de la nécessité d'observer des obligations juridiques internationales » (Cour eur. D.H., *Parti communiste unifié de Turquie et autres c. Turquie*, 30 janvier 1998, § 29).

[24] C.J.U.E., 3 septembre 2008, arrêt *Kadi et Al Barakaat International Foundation c. Conseil et Commission*, C-402/05 P et C-415/05 P, § 283.

[25] S. Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E. », *op. cit.*, p. 227.

protection de données de portée potentiellement mondiale[26], pose les principes généraux relatifs à la protection des données à savoir, les principes de loyauté, de licéité, de finalité, de qualité et de proportionnalité tout en admettant certaines dérogations dans le cadre de la lutte contre « la répression des infractions pénales »[27].

11. Particulièrement importante pour notre propos, la recommandation R (87) 15 vise à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[28] tout en s'inspirant des principes retenus par la Convention 108. Depuis son adoption, cette recommandation a fait l'objet de plusieurs évaluations (en 1993, 1998 et 2002). En 2010, le Comité consultatif de la Convention 108 a décidé de réaliser une étude sur l'utilisation de données à caractère personnel dans le secteur de la police dans l'ensemble de l'Europe. Cette évaluation a montré qu'elle constituait toujours un point de départ approprié pour élaborer des réglementations en droit national[29]. Il fut alors suggéré d'émettre un instrument contraignant susceptible d'être déployé dans des secteurs jusqu'alors souvent parallèles : celui des forces de police et celui des agences de sécurité et de renseignement[30].

12. Avec l'entrée en vigueur du Traité de Lisbonne en 2009, la Charte des droits fondamentaux de l'Union européenne a acquis force juridique

---

[26] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *STCE*, n° 108, 1981.

[27] Art. 9 de la Convention 108. Notons que cette Convention fait l'objet d'un protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données. Ce texte prévoit tout d'abord l'établissement d'autorités de contrôle chargées d'assurer le respect des lois ou règlements introduits par les États en application de la Convention concernant la protection des données personnelles et les flux transfrontières de données. Le deuxième point concerne les flux transfrontières de données vers des pays tiers, qui ne pourront être transférées que si elles bénéficient dans l'État ou l'organisation internationale destinataire, d'un niveau de protection adéquat. *Voy.* Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, *STCE*, n° 181, Strasbourg, 8 novembre 2001.

[28] Comité des Ministres du Conseil de l'Europe, Recommandation R (87)15 du 15 septembre 1987 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (ci-après Recommandation R (87)15).

[29] Conseil de l'Europe, rapport « Recommandation (87)15 – Vingt-cinq ans après - rapport final », Strasbourg, 18 février 2014.

[30] Notons que suite à cette évaluation, le Conseil de l'Europe a élaboré un guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police fournissant des éléments d'orientation sur l'implication de ces pratiques au niveau opérationnel (Comité consultatif de la Convention pour la protection des données des personnes à l'égard du traitement automatisé des données à caractère personnel, « Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police », Strasbourg, 15 février 2018).

obligatoire[31] et le droit à la protection des données à caractère personnel[32] a été érigé au rang de droit fondamental autonome[33]. Cette constitutionnalisation de la Charte a offert un terrain neuf à la Cour de justice de l'Union européenne s'émancipant progressivement de la jurisprudence de la Cour de Strasbourg. Elle a peu à peu développé une conception autonome du droit à la protection des données[34] teintée par des décisions considérées à maintes égard comme historiques[35].

13. Dans le cadre du train de mesures législatives visant à réformer la législation de l'Union sur la protection des données, une proposition de directive applicable au secteur de la « police » et de la « justice » fut déposée en décembre 2012[36]. Après trois années de négociations, la directive 2016/680/UE a été adoptée en 2016 et doit être transposée au sein des États membres pour le 6 mai 2018[37]. Calquée sur la structure et logique du RGPD, elle fixe un corps de règles de protection des données adapté au domaine pénal afin de favoriser la libre circulation de ces données au sein de l'Union et assurer une meilleure efficacité relative à la coopération

[31] Art. 6, § 1, TUE, *J.O.*, C 326 du 26 octobre 2012.

[32] Précisons par ailleurs que selon l'article 8, § 2, de la Charte, les « données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ». L'article 52, § 1, de la Charte autorise les États membres à limiter la portée des droits et libertés par la voie législative pour autant que la mesure respecte le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elle soit nécessaire et réponde effectivement à un objectif d'intérêt général reconnu par l'Union.

[33] Art. 16 TFUE.

[34] S. Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E. », *op. cit.*, p. 229.

[35] Voy. entres autres : C.J.U.E., 6 octobre 2015, arrêt *Schrems c. Data Protection Commissionner of Ireland,* C-362/14 ; C.J.U.E., 8 avril 2014, arrêt *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12 ; C.J.U.E., 21 décembre 2016, arrêt *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.,* affaires jointes C-203/15 et C-698/15, § 110 ; C.J.U.E., 26 juillet 2017, avis 01/2015.

[36] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012)0010, 25 janvier 2012.

[37] Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *OJ*, L 119 du 4 mai 2016, pp. 89-131 (ci-après directive 2016/680).

judiciaire et policière[38]. Dans l'esprit du Traité de Lisbonne[39], elle vise également à protéger les libertés et droits fondamentaux des personnes physiques et en particulier, leur droit à la protection des données[40] tout en laissant la possibilité aux États membres de prévoir des garanties plus étendues pour les personnes concernées[41].

CHAPITRE 2. Champ d'application matériel

14. La directive 2016/680/UE s'applique à tout « traitement de données à caractère personnel par les autorités compétentes dans le domaine de la prévention et la détection des infractions pénales, les enquêtes et poursuites en la matière ainsi que l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données »[42].

15. Les « autorités compétentes » visées ne sont pas uniquement les autorités publiques telles les autorités policières ou judicaires, mais comprennent de manière large tout organisme ou entité publique et/ou privée disposant, en vertu d'une base légale, de prérogatives de puissance publique dans le cadre des finalités visées par la directive[43]. Ainsi, lorsque la gestion des prisons est confiée à une entreprise privée, celle-ci est soumise à la directive 2016/680/UE lorsqu'elle agit dans le cadre des finalités visées par celle-ci. En revanche, un établissement financier ou un opérateur de voyage, traitant des données à caractère personnel à des fins

[38] Considérants n^{os} 7 et 25 de la directive 2016/680/UE et CEPD, avis n° 6/2015, Une nouvelle étape vers une protection européenne complète de données, recommandations du CEPD sur la directive pour la protection des données dans les secteurs police et justice, 28 octobre 2015, p. 5 (ci-après CEPD, avis n° 6/2015).

[39] Comme le rappelle le considérant n° 10 de la directive 2016/680, dans la déclaration n° 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée au Traité de Lisbonne, « la conférence a reconnu que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière » pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines ».

[40] Art. 1, § 2, a, de la directive 2016/680/UE.

[41] Art. 1, § 3, de la directive 2016/680/UE.

[42] Art. 1, § 1, de la directive 2016/680/UE.

[43] Considérant n° 11 de la directive 2016/680/UE. Selon le même considérant, si cet organisme ou entité agit en tant que sous-traitant, il devrait être lié par un contrat ou un autre acte juridique et par les dispositions applicables aux sous-traitants.

commerciales et fournissant certaines de ces données sur demande des autorités ou en vertu d'une obligation légale, est tenu de se conformer aux dispositions du RGPD[44]. De même, lorsqu'une société privée obtempère au transfert de données sur la base d'une obligation de collaboration dans le cadre d'une enquête pénale cette dernière reste tenue de respecter les dispositions du RGDP tandis que le traitement effectué par l'autorité publique est soumis à la directive 2016/680/UE[45].

Par ailleurs, a l'instar des autorités répressives, les juridictions et les autorités judiciaires sont soumises au respect des dispositions relatives à la directive 2016/680/UE, notamment lorsqu'elles traitent des données à caractère personnel dans les décisions judiciaires ou les documents relatifs aux procédures pénales[46]. Ceci ne prive toutefois pas les États membres de la possibilité de préciser les opérations et les procédures de traitement dans leurs règles de procédures pénales[47]. Notons en outre que la directive exclut de son champ d'application les traitements de données à caractère personnel par les institutions de l'Union, organismes, bureaux et agences[48].

16. La notion d'infraction « pénale » au sens de la directive 2016/680/UE est une notion autonome, interprétée à la lumière de la jurisprudence de la C.J.U.E[49]. et indépendamment du droit des États membres, assurant une certaine interprétation uniforme du droit de l'Union[50]. La qualification pénale d'une infraction en droit interne n'est donc pas déterminante pour définir le champ d'application de la directive, celle-ci visant l'ensemble des infractions – qu'elles soient pénales ou administratives – donnant lieu à des sanctions recouvrant un caractère « punitif et dissua-

[44] Art. 9, § 1, et considérant n° 11 de la directive 2016/680/UE.

[45] Une société privée peut être occasionnellement tenue, en vertu d'une obligation légale, d'une mission d'intérêt public, telle que l'injonction de produire certaines données dans le cadre d'une enquête pénale. En ce cas, l'autorité publique n'est pas considérée comme un « destinataire » de ces données au sens de l'article 4, § 9, du RGPD et dès lors, ne doit pas apparaitre dans le registre des activités de traitement du responsable du traitement. En outre, le transfert de ces données est licite dans la mesure où il est considéré comme relevant de l'intérêt légitime du responsable du traitement. Voy. considérant n° 50 du RGPD.

[46] Considérant n° 20 de la directive 2016/680/UE.

[47] Considérant n° 20 de la directive 2016/680/UE.

[48] Art. 2, § 3, de la directive 2016/680/UE.

[49] Considérant n° 13 de la directive 2016/680/UE.

[50] Comme le souligne la C.J.U.E. à l'égard du respect de la règle *ne bis in idem* : « Même en l'absence d'harmonisation des législations pénales des États membres, l'application uniforme du droit de l'Union requiert, selon une jurisprudence constante, qu'une disposition ne renvoyant pas au droit de ces États reçoive une interprétation autonome et uniforme, qui doit être recherchée en tenant compte du contexte de la disposition dans laquelle elle s'insère et de l'objectif poursuivi ». C.J.U.E., 27 mai 2014, arrêt *Zoran Spasic*, C-129/14 PPU, § 79.

sif »[51]. Précisons également que le traitement des données relatives aux condamnations pénales, aux infractions pénales et aux mesures de sûreté connexes sont encadrées de manière spécifique par le RGDP lequel les soumet au contrôle de l'autorité publique[52].

17. La « prévention des infractions pénales » vise les données collectées dans le cadre d'une enquête spécifique mais aussi les données traitées par les autorités au-delà de ce cadre, pour acquérir une meilleure compréhension de certains phénomènes[53]. Ainsi, l'étude de facteurs sociaux, psychologiques et économiques permettant d'établir des statistiques relatives au comportement menant au crime organisé et au terrorisme par exemple, tombe dans le champ d'application de la directive.

18. Outre les infractions pénales et leur prévention, la directive 2016/680/UE s'applique aux traitements effectués dans le cadre de « la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »[54], c'est-à-dire les activités menées par la police ou par les autorités répressives à des fins de maintien de l'ordre public entre autres lors de manifestations, de grands événements sportifs et d'émeutes[55] et ce, sans savoir au préalable si un incident constitue une infraction pénale ou non[56]. Cet élargissement par rapport au champ d'application de la décision-cadre 2008/977 a fait l'objet de critiques du CEPD considérant que cette disposition « ne permet pas une délimitation claire des tâches de la police relevant du champ d'application de la directive ». À titre illustratif, le suivi d'une tentative de suicide peut aussi bien concerner la sécurité publique que la santé[57]. De même, selon le Groupe 29, la prévention des menaces contre la sécurité publique pris indépendamment de la notion d'« infraction pénale » est un concept vague pouvant inclure un nombre indéfini de situations occasionnellement liées à cet objectif, certains États

[51] Ces critères ont notamment été retenus par la C.J.U.E. à l'égard de la reconnaissance mutuelle des sanctions pécunières infligées en cas d'infraction routière. Voy. C.J.U.E., 14 novembre 2013, arrêt *Baláž*, C-60/12, § 35. La Cour eur. D.H. applique le « test Engel » et prend en considération les critères suivants : la qualification de l'infraction en droit national, la nature de l'infraction et le degré de gravité de la sanction infligée. L'objectif est d'éviter qu'une personne puisse être poursuivie sans bénéficier des protections découlant d'une procédure pénale au motif d'être qualifiée de procédure administrative par le législateur par exemple. Cour eur. D.H., 8 juin 1976, *Engel et al. c. Pays-Bas*, série A, n° 22.

[52] Art. 10 du RGPD.

[53] Considérant n° 27 de la directive 2016/680/UE.

[54] Art. 1 de la directive 2016/680/UE.

[55] Considérant n° 12 de la directive 2016/680/UE.

[56] Considérant n° 12 de la directive 2016/680/UE.

[57] CEPD, avis n° 6/2015, p. 6.

incluant par exemple la santé publique dans la sécurité publique[58]. L'un comme l'autre recommandaient dès lors de limiter le champ d'application de la directive aux activités relevant du droit pénal au risque d'aboutir des régimes de protection des données distincts selon les États membres.

19. La référence à la notion de « menace » laisse penser que la directive 2016/680/UE pourrait également s'appliquer au traitement de données relatif à la sécurité nationale intérieure. En principe, ce domaine reste de la seule responsabilité de chaque État membre de sorte que l'UE n'est pas compétente pour légiférer en la matière[59]. En ce sens, le considérant n° 14 de la directive 2016/680/UE indique exclure de son champ d'application les activités qui ne relèvent pas du droit de l'Union, telles les activités des agences ou des services responsables des questions de sécurité nationale[60]. Cependant, ni le droit de l'UE, ni la jurisprudence de la C.J.U.E. n'offrent une définition claire de ce que revêt le terme « sécurité nationale »[61]. Différents traités de l'UE y font toutefois référence, ou font référence à des notions étroitement liées telles la sécurité intérieure, la sûreté de l'État et la défense, domaines pour lesquels l'UE est habilitée à légiférer[62]. Sur cette base, les législateurs nationaux pourraient décider d'inclure ou non les activités des services de renseignement dans le champ d'application de leur loi transposant la directive 2016/680/UE.

20. Selon le Groupe 29, pour déterminer ce qu'il y a lieu d'entendre par « sécurité nationale », il convient de tenir compte de la situation politique et des acteurs concernés[63] sans que cette exclusion ne puisse servir d'excuse aux États membres pour refuser d'appliquer la législation

[58] Groupe 29, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP 233, 1er décembre 2015, p. 5 (ci-après Groupe 29, Avis 03/2015).

[59] Art. 4, § 2, TUE.

[60] Considérant n° 14 de la directive 2016/680/UE.

[61] De son côté, la Cour eur. D.H. a estimé que la notion de « sécurité nationale » ne pouvait recevoir de définition exhaustive, lui conférant une certaine élasticité et une certaine flexibilité reflétée par la marge d'appréciation dont jouissent les États membres en la matière. Cour eur. D.H., 2 avril 1993, *Esbester c. Royaume-Uni*, n° 18601/91.

[62] Groupe 29, Document de travail sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, WP 228, 5 décembre 2014, p. 23. L'exemple le plus couramment cité est celui de la lutte contre le terrorisme. Voy. directive 2017/541/UE relative à la lutte contre le terrorisme, *J.O.*, L 88 du 31 mars 2017, p. 6.

[63] Groupe 29, Document de travail sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, WP 228, 5 décembre 2014, p. 23.

relative à la protection des données[64]. Dans le même sens, pour le CEPD, le concept de « sécurité nationale » doit être défini en référence à la politique nationale des États membres et ne pourrait servir de prétexte « pour légitimer le traitement de données à caractère personnel en dehors du champ d'application du règlement et de la directive, par exemple dans le cadre de la lutte contre le terrorisme »[65]. Il incombe donc aux États membres d'appliquer ou de refuser d'appliquer la directive 2016/680/UE aux activités des services de renseignements ou de la Sûreté de l'État eu égard à leur système constitutionnel. Concrètement, on peut déjà noter que la Belgique inclut dans son projet de loi assurant la transposition de la directive 2016/680/UE et du RGPD les activités des services de renseignement sans toutefois faire référence à la directive en ce qui les concerne. Le Luxembourg fait, quant à lui, directement référence à la directive 2016/680/UE mais complète dans son projet de loi les finalités visées par « menaces pour la sécurité nationale et prévention de telles menaces »[66] tandis que la France s'y refuse considérant que la directive n'est pas applicable « aux traitements intéressant la sûreté de l'État et la défense, qui ne relèvent pas du droit de l'Union européenne »[67].

CHAPITRE 3. Principes relatifs aux traitements de données à caractère personnel

SECTION 1. – Principes de licéité et de loyauté

21. Selon l'article 8 de la directive 2016/680/UE, un traitement est licite « dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er,

[64] *Ibid.*, p. 27.

[65] CEPD, avis n° 6/2015, p. 6.

[66] Projet de loi n° 7168 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification et portant modification de certaines lois. Le projet de loi est censé transposer la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[67] Projet de loi relatif à la protection des données personnelles (JUSC1732261L).

paragraphe 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre ». La directive ne reprend donc pas les six bases légales du RGPD[68]. En effet, requérir le consentement de la personne concernée aurait peu de sens dans le domaine pénal et celui de la justice où cette dernière est généralement tenue d'obtempérer au traitement de ses données et ne dispose donc pas réellement d'une véritable liberté de choix[69]. En revanche, la directive prévoit que le consentement de la personne concernée peut être requis en tant que garantie supplémentaire, en cas de traitement de données particulièrement sensibles par exemple[70], ou pour pouvoir effectuer un test ADN dans le cadre d'une enquête ou encore, en vue de permettre un dispositif de surveillance électronique par le biais d'une géolocalisation dans le cadre de l'exécution de sanctions pénales[71]. En ce cas, la personne doit être informée de manière claire et non ambiguë de la possibilité de retirer son consentement à tout moment[72].

22. Précisons que la base juridique ne doit pas forcément être un acte législatif émanant du Parlement mais doit être qualifiable de « claire, prévisible et accessible » conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme[73]. La réglementation doit néanmoins indiquer au minimum les objectifs poursuivis, les finalités du traitement, les données à caractère personnel qui font l'objet d'un traitement, les procédures pour garantir l'intégrité et la confidentialité des données à caractère personnel ainsi

[68] Art. 6 du RGPD.

[69] Considérant n° 35 de la directive 2016/680/UE. Cette approche rejoint celle du RGPD selon laquelle le consentement ne peut être donné librement et constituer une base juridique valable pour le traitement de données à caractère personnel « lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière ». Considérant n° 43 du RGPD.

[70] Selon le considérant n° 37 de la directive 2016/680, le traitement des données sensibles exige le respect des garanties appropriées pour les droits et libertés de la personne concernée mais aussi, le traitement de ces données devrait être autorisé par la loi « lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes ».

[71] Considérant n° 35 de la directive 2016/680/UE.

[72] Groupe 29, Opinion on some key issues of the Law Enforcement (EU 2016/680), WP 258, 29 novembre 2017, p. 9 (ci-après Groupe 29, Avis 2017)

[73] Considérant n° 35 de la directive 2016/680/UE. Voy. not. : Cour eur. D.H., 2 août 1984, *Malone c. Royaume-Uni*, série A, n° 82, § 67 ; C.J.U.E., 17 décembre 2015, *WebMindLicenses,* C-419/14, § 81.

que les procédures prévues pour la destruction de celles-ci, fournissant dès lors des garanties suffisantes vis-à-vis des risques d'utilisation abusive et arbitraire[74].

SECTION 2. – Principe de finalité

23. Le principe de la limitation de la finalité, pierre angulaire du régime de la protection des données[75], permet de concrétiser celui de la minimisation des données : il s'agit premièrement de comprendre pourquoi des données sont traitées avant de pouvoir déterminer celles qui doivent l'être afin d'éviter le risque d'en traiter davantage que nécessaire pour atteindre l'objectif poursuivi[76]. À l'instar des règles prévues par le RGPD, les données traitées par les autorités compétentes doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent être traitées d'une manière incompatible avec ces finalités[77].

24. De plus, en ce qui concerne l'évaluation de la compatibilité des traitements ultérieurs, par le responsable du traitement ou par un autre, dans le cadre des finalités visées par la directive, l'article 4, § 2, de la directive 2016/680/UE requiert que ce traitement soit autorisé par le droit de l'Union ou par le droit d'un État membre et qu'il soit nécessaire et proportionné au regard de cette autre finalité[78]. Ainsi, le ministère public traitant certaines données à caractère personnel dans le cadre d'une enquête peut réutiliser ces données après la condamnation de la personne concernée dans le cadre de l'exécution des peines. En cas de transferts entre autorités répressives au sein de l'UE, l'autorité assurant le transfert est tenue d'informer le destinataire des conditions du traitement et de l'obligation de les respecter, par exemple, un éventuel *code de traitement* ou d'interdire de transmettre les données ultérieurement à autrui[79].

25. En outre, lorsqu'une autorité compétente collecte des données dans le cadre des finalités visées par la directive 2016/680/UE et les traite

[74] Art. 8, § 2, et considérant n° 35 de la directive 2016/680/UE.

[75] Groupe 29, Avis 03/2013 sur la limitation des finalités, 3 avril 2013.

[76] Groupe 29, Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, 27 février 2014, pt 5.7. Voy. égal. CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017.

[77] Art. 4, § 1, b, de la directive 2016/680/UE et art. 5 du RGPD.

[78] Considérant n° 29 de la directive 2016/680/UE.

[79] Art. 9, § 3, et considérant n° 36 de la directive 2016/680/UE.

ultérieurement à d'autres fins, conformément au droit de l'Union ou d'un État membre, le RGDP est applicable, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union[80]. Ainsi, lorsque les services de police collectent certaines données pour traiter les plaintes de victimes, ils sont tenus au respect de la directive. Par contre, s'ils réutilisent ces données pour une estimation du montant des aides qui pourrait être rétribué aux victimes, ils doivent se soumettre aux dispositions du RGDP. À ce propos, le CEPD soulignait le danger d'un traitement ultérieur ayant une finalité totalement différente et recommandait « d'ajouter des éléments supplémentaires au texte afin de délimiter la notion de limitation de la finalité dans le domaine de la police et de la justice et de préciser la notion de traitement ultérieur incompatible »[81]. Il prenait pour exemple le risque que des données collectées à des fins policières puissent être traitées ultérieurement à des fins d'immigration[82]. Un autre exemple qui pose question est celui des flux de données entre services de renseignement et services de police lesquels poursuivent des missions différentes[83].

SECTION 3. – Principe d'exactitude

26. De manière similaire aux dispositions prévues par le RGDP, les données à caractère personnel traitées dans le cadre des finalités visées par la directive 2016/680/UE, doivent être exactes et si nécessaire, mises à jour en prenant toutes les mesures raisonnables pour que les données inexactes ou incomplètes soient effacées ou rectifiées[84]. Plus spécifiquement, et dans la lignée de la Recommandation R (87)15[85], les données doivent être catégorisées en fonction de leur degré d'exactitude ou de fiabilité[86]. Autrement dit, les données « fondées sur des faits » doivent

[80] Art. 9, § 1, de la directive 2016/680/UE.

[81] CEPD, avis n° 6/2015, p. 7.

[82] CEPD, avis n° 6/2015, p. 7.

[83] Ce mélange de finalités est illustré dans le domaine des surveillances des communications électroniques par le Groupe 29 relevant qu'il « conviendrait de déterminer dans quelle mesure une ingérence fondée sur la sécurité nationale demeure le reflet de la réalité, maintenant qu'il apparaît que le travail des services de renseignement est plus que jamais interconnecté avec celui des autorités répressives et qu'il poursuit plusieurs objectifs différents ». voy. Groupe 29, Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, WP 215, 10 avril 2014, p. 16.

[84] Art. 4, d, de la directive 2016/680/UE et art. 5, d, du RGPD.

[85] Considérant n° 30 de la directive 2016/680/UE.

[86] Art. 7, § 1, de la directive 2016/680/UE.

« dans la mesure du possible » être distinguées de « celles fondées sur des appréciations personnelles » à la lumière de la nature et de la finalité du traitement[87]. Cette obligation de catégorisation est une obligation de moyen dans la mesure où la fiabilité ou l'exactitude de certaines données peut dépendre de l'évolution d'une enquête, par exemple, les témoignages, l'appréciation des pièces d'un dossier, le statut de victime ou de témoin.

SECTION 4. – La durée de conservation des données

27. Les données ne peuvent être conservées « sous une forme permettant l'identification des personnes concernées » pour une durée supérieure à celle nécessaire au regard de l'objectif poursuivi[88]. À ce propos, la C.J.U.E. a rappelé à plusieurs reprises que la période conservation des données devait « toujours répondre à des critères objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi »[89].

28. La directive 2016/680/UE confie aux législateurs nationaux de fixer, via des règles procédurales, les délais appropriés pour l'effacement des données à caractère personnel et/ou d'organiser un examen périodique portant sur la nécessité de conserver les données compte tenu de l'objectif poursuivi[90]. Selon le Groupe 29, cette formulation laisse la porte ouverte à la mise en place de système mixte c'est-à-dire un système fixant des délais de conservation maximaux généraux couplé avec un examen périodique spécifique permettant soit de conserver certaines données pendant une période supplémentaire[91], soit de conserver les données en vue d'un traitement à d'autres fins dans les conditions prévues par la

[87] Considérant n° 30 de la directive 2016/680/UE.

[88] Art. 4, e, de la directive 2016/680/UE.

[89] C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland,* C-362/14, § 93 ; C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.,* affaires jointes C-203/15 et C-698/15, § 110.

[90] Art. 5 et considérant n° 26 de la directive 2016/680/UE. À titre illustratif, la Cour européenne des droits de l'homme a considéré que la conservation de données à caractère personnel relatives à des faits ayant été classés sans suite pendant une durée de vingt ans entrainait une ingérence disproportionnée dans le droit au respect de la vie privée. Cour eur. D.H., 18 septembre 2014, *Brunet c. France*, n° 21010/10.

[91] Groupe 29, Avis 2017, p. 3.

directive[92]. Dans le cas où les données sont traitées à des fins préventives par exemple, un examen périodique pourra permettre de vérifier si le stockage des données est toujours nécessaire, d'autant qu'à la différence des données traitées dans le cadre d'une enquête pénale, aucune décision définitive n'impliquera la suppression automatique des données collectées[93].

En outre, le Groupe 29 recommande de lire l'article 5 en combinaison avec l'article 6 et de prévoir un régime graduel du stockage des données en fonction des catégories de personnes concernées, telles les victimes, témoins, suspects ou tiers, mais aussi de prévoir des garanties supplémentaires au fil et à mesure du temps, par exemple, en renforçant les conditions d'accès aux données en fonction de l'objectif poursuivi[94].

SECTION 5. – Le principe de sécurité des données

29. Les données doivent être traitées de « façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées »[95]. Cette obligation de sécurité imposée au responsable du traitement des données et au sous-traitant, se décline en une multitude de sous-obligations relativement similaires à celles contenues dans le RGPD[96]. Cet alignement vise à assurer une certaine cohérence entre les deux textes permettant d'éviter des chevauchements ou confusions susceptibles d'amoindrir le degré de protection

[92] L'article 4, § 3, de la directive 2016/680/UE précise que « le traitement des données par le même ou par un autre responsable du traitement peut comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 1er, paragraphe 1, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée » et l'article 9, § 1, énonce que : « les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1er, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1er, paragraphe 1, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union ou le droit d'un État membre. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union ».

[93] Groupe 29, Avis 2017, p. 4.

[94] Groupe 29, Avis 2017, p. 5.

[95] Art. 4, f, de la directive 2016/680/UE.

[96] Pour le RGPD voy. chapitre IV, art. 24 et s.

des données offert aux personnes concernées[97]. Selon le Groupe 29, ce parallélisme est essentiel compte tenu de l'intensification des échanges entre les autorités répressives et les administrations ou autorités publiques agissant à d'autres fins que celles visées par la directive 2016/680/UE mais aussi entre les entités privées et les autorités répressives[98].

30. En conséquence, le responsable du traitement et le sous-traitant sont tenus d'adopter des mesures techniques et organisationnelles appropriées[99] et en particulier, de prévoir des règles internes relatives aux principes de « protection des données dès la conception » et « protection des données par défaut »[100], d'avoir recours à la pseudonymisation[101], de tenir un registre des « catégories » d'activités de traitement effectuées sous leur responsabilité[102] (et non des activités de traitement comme le prévoit le RGPD)[103] et de désigner un délégué à la protection des données[104] tout en considérant que les juridictions agissant dans l'exercice de leur fonction juridictionnelle peuvent en être dispensées[105]. Par ailleurs, en cas de violation de données à caractère personnel, le responsable du traitement doit notifier l'incident à l'autorité de contrôle dans un délai de 72 heures après la prise connaissance, à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et les libertés d'une personne physique[106]. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard[107].

31. Concernant l'analyse d'impact relative à la protection des données, les dispositions du RGDP ainsi que les lignes directrices développées

---

97 Groupe 29, Avis 03/2015, p. 4.

98 Groupe 29, Avis 03/2015, p. 4.

99 Selon le considérant n° 28 de la directive 2016/680/UE : « Afin de préserver la sécurité entourant le traitement et de prévenir tout traitement effectué en violation de la présente directive, il convient que les données à caractère personnel soient traitées de manière à garantir un niveau de sécurité et de confidentialité approprié, notamment en empêchant l'accès non autorisé à ces données et à l'équipement servant à leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement, et à tenir compte de l'état des connaissances et de la technologie disponible, des coûts de mise en œuvre au regard des risques et de la nature des données à caractère personnel à protéger ».

100 Art. 20 et considérants n^{os} 52 et 53 de la directive 2016/680/UE et art. 25, § 1, du RGPD.

101 Art. 3, 10, de la directive PNR.

102 Art. 24 et considérant n° 56 de la directive 2016/680/UE.

103 Art. 30 du RGPD.

104 Art. 32 de la directive 2016/680/UE et art. 37 du RGPD.

105 Considérant n° 63 de la directive 2016/680/UE.

106 Art. 30, § 1, de la directive 2016/680/UE.

107 Art. 30, § 1, de la directive 2016/680/UE.

par le Groupe 29[108] s'appliquent *mutatis mutandis* pour l'interprétation des dispositions de la directive 2016/680[109]. Il incombe donc au responsable du traitement d'effectuer une analyse d'impact des opérations de traitement envisagées lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques compte tenu de la nature, de la portée, du contexte et des finalités du traitement[110]. Cette analyse doit porter sur les systèmes et processus pertinents des opérations de traitement tels des fichiers, et non sur des cas individuels[111]. Elle doit ensuite être fournie à l'autorité de contrôle, sur demande ou dans le cadre d'une consultation préalable, afin de lui permettre d'apprécier la conformité du traitement et les risques pour les droits et liberté des personnes physiques[112].

32. Par ailleurs, lorsque le traitement des données à caractère personnel fera partie d'un nouveau « fichier »[113] à créer, le responsable du traitement ou le sous-traitant doit consulter préalablement l'autorité de contrôle dans deux cas. Cette consultation est tout d'abord prévue si l'analyse d'impact indique que le traitement pourrait présenter un risque élevé dans le cas où le responsable du traitement ne prendrait pas de mesures pour atténuer le risque. Elle doit également intervenir si le type de traitement, en particulier, compte tenu de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées[114].

Si l'autorité de contrôle estime que le traitement pourrait entraîner une violation des dispositions adoptées en vertu de la directive, elle fournit un avis par écrit dans un délai maximum de six semaines à compter de la réception de la demande de consultation mais peut aussi adopter des mesures correctrices dans les conditions prévues par l'article 47 de la directive

---

[108] Groupe 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendre un risque élevé » aux fins du règlement (UE) 2016/679, 4 avril 2017.

[109] Groupe 29, Avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale p. 6 ; Commission de la protection de la vie privée, Recommandation n° 01/2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable, 28 février 2018.

[110] Art. 27, § 1, de la directive 2016/680/UE et art. 35, § 1, du RGPD.

[111] Considérant n° 58 de la directive 2016/680/UE.

[112] Art. 28, § 4 de la directive 2016/680/UE.

[113] Selon l'article 3, § 6, de la directive, un fichier est défini comme « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

[114] Art. 28, § 1, de la directive 2016/680/UE.

2016/680/UE et telles que détaillées *infra*[115]. L'autorité de contrôle doit également être consultée dans le cadre de l'élaboration d'une proposition de mesure législative[116] mais aussi en vertu d'une liste des opérations de traitement qu'elle peut établir[117]. En outre, l'article 29, § 2, de la directive 2016/680/UE liste une série de mesures techniques et organisationnelles à mettre en œuvre par le responsable du traitement ou le sous-traitant, en cas de traitement automatisé, à la suite d'une évaluation des risques[118].

33. Remarque importante, à la différence du RGPD, la directive 2016/680/UE impose expressément la tenue de journaux dans le cadre de différentes opérations telles la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement de données[119]. Ces journaux doivent indiquer le motif, la date et l'heure de l'opération et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données[120]. Ils doivent être mis à disposition de l'autorité de contrôle, sur demande[121] afin qu'elle

115 Art. 28, § 5, de la directive 2016/680/UE.

116 Art. 28, § 2, de la directive 2016/680/UE.

117 Art. 28, § 3, de la directive 2016/680/UE.

118 Les mesures reprises par l'article 29, § 2, de la directive sont les suivantes : (a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ; (b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données) ; (c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation) ; (d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ; (e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données) ; (f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission) ; (g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction) ; (h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport) ; (i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ; (j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

119 Art. 25, § 1, de la directive 2016/680/UE.

120 Art. 25, § 1, de la directive 2016/680/UE.

121 Art. 25, § 3, de la directive 2016/680/UE.

puisse vérifier la licéité de certaines opérations, d'effectuer des autocontrôles en ce compris dans le cadre de procédures disciplinaires internes des autorités compétentes[122]. Ils permettent également de garantir l'intégrité et la sécurité des données dans le cadre de procédures pénales[123], par exemple lorsque la légalité d'une opération de traitement de données est contestée ou lorsqu'une violation de données à caractère personnel est en jeu[124]. Comme le souligne le Groupe 29, l'implémentation des logs est un outil crucial en protection des données puisqu'il permet de contrôler les opérations effectuées, de retracer l'activité des utilisateurs et de détecter les utilisations abusives[125]. L'enregistrement des fichiers logs peut à la fois recouvrir un aspect dissuasif et un aspect sanctionnateur[126]. À nouveau, conformément au principe de protection des données dès la conception, il convient de prendre en considération ces exigences lors de la conception des applications et en particulier, du régime d'accès à la base de données, au système ou à l'application[127]. Le Groupe 29 rappelle en outre qu'il revient aux législateurs nationaux de prévoir des périodes de conservation des logs sur base de critères clairs ou en fixant des périodes fixes en fonction des objectifs visés[128].

CHAPITRE 4. Catégories de personnes concernées

34. Conformément à la Recommandation R (87)15 et, à la différence du régime prévu par la décision-cadre 2008/977, l'article 6 de la directive 2016/680/UE impose au responsable du traitement de prévoir des catégories de données en fonction des personnes concernées. Doivent donc être distinguées, les données des personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale, les personnes reconnues coupables d'une infraction pénale et les victimes ou les personnes dont les faits portent à croire qu'elles pourraient être victimes d'une infraction pénale[129].

122 Considérant n° 57 de la directive 2016/680/UE.
123 Art. 25, § 2, de la directive 2016/680/UE.
124 Groupe 29, Avis 2017, p. 27.
125 Groupe 29, Avis 2017, p. 26.
126 Groupe 29, Avis 2017, p. 26.
127 Groupe 29, Avis 2017, p. 27.
128 Groupe 29, Avis 2017, p. 27.
129 Considérant n° 31 de la directive 2016/680/UE.

Les tiers à une infraction pénale, autres que les témoins ou les personnes susceptibles de pouvoir fournir des informations aux enquêteurs, ont fait l'objet d'une attention particulière du Groupe 29, ce dernier estimant que le traitement de leurs données devrait être limité à celui « nécessaire à l'enquête relative à une infraction pénale spécifique ou aux poursuites y afférentes » et pour autant qu'il soit « indispensable à des fins préventives ciblées ou à des fins d'analyse criminelle, si et aussi longtemps que ces fins sont légitimes, clairement définies et spécifiques »[130]. À titre illustratif, le système « PNR » pour Passenger Name Records vise cette catégorie spécifique de tiers en imposant aux transporteurs de voyage le transfert systématique des données des passagers aux autorités compétentes en vue d'évaluer les risques potentiels que ces passagers pourraient présenter pour la sécurité publique. Ce mécanisme a été fortement critiquée par le Conseil de l'Europe considérant qu'il s'applique à des personnes « qui n'ont commis aucune infraction » et qu'il ne pourrait en aucun cas viser « un but légitime » d'autant qu'il existe un risque d'erreur inévitable susceptible de mener à du profilage discriminatoire[131]. Néanmoins, dans le cadre de l'examen de l'accord PNR conclu entre le Conseil de l'Union et le Canada[132], la C.J.U.E. a validé un outil de « renseignement en matière criminelle »[133] s'appliquant à des tiers, sous réserve de règles matérielles et procédurales strictes et notamment, l'exclusion des finalités vagues et générales[134] rencontrant dès lors les exigences précitées du Groupe 29.

---

[130] Groupe 29, Avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale, p. 4.

[131] Ces critiques ont notamment été rédigées à l'occasion de la proposition de directive « PNR » (directive 2016/681/UE du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *OJ*, L 119 du 4 mai 2016, pp. 132–149) Voy. en ce sens le rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, *Passenger Name Records, data mining & data protection : the need for strong safeguards*, 15 juin 2015, T-PD(2015)11). La directive PNR a également été critiquée par le CEPD (avis du CEPD n° 5/2015, *Deuxième avis sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière*, 24 septembre 2015, p. 9).

[132] C.J.U.E., 26 juillet 2017, avis 01/2015.

[133] Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (COM/2011/0032 final).

[134] C.J.U.E., 26 juillet 2017, avis 01/2015, § 181.

CHAPITRE 5. Catégories particulières de données

35. Les données relevant de ces catégories particulières et dites « sensibles » sous le régime de la directive 95/46/CE, sont les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique[135]. Les données génétiques et biométriques telles que les empreintes digitales et l'ADN, aux fins d'identifier une personne physique, sont désormais expressément définies et incluses dans la catégorie des données sensibles[136]. Compte tenu des risques pour les droits et libertés des personnes physiques, le RGDP interdit le traitement de ces données, sauf exceptions[137]. La directive 2016/680/UE par contre, autorise le traitement de ces données sous réserve de certaines conditions[138] et ce, en dépit de l'avis contraire du CEPD[139] et de la Recommandation R (87)15[140].

36. Ainsi, le traitement des données sensibles doit être « absolument nécessaire »[141], être assorti de garanties appropriées et être autorisé par le droit de l'Union ou par le droit d'un État membre[142]. Deux exemples sont visés par la directive à savoir d'une part, la situation où les intérêts vitaux d'une personne sont en jeu[143] et d'autre part, lorsque les données sont manifestement rendues publiques par la personne concernée[144] qu'elles soient publiées dans une biographie, dans la presse ou sur un site Web

---

[135] Art. 10 de la directive 2016/680/UE.

[136] C. JASSERAND, « Legal Nature of Biometric Data : From "Generic" Personal Data to Sensitive Data », *EDPL*, 2016/3, pp. 297-311.

[137] Art. 9 RGPD.

[138] Art. 10 de la directive 2016/680/UE.

[139] CEPD, avis n° 6/2015, p. 7.

[140] Principe 2 de la Recommandation R (87)15.

[141] Selon le Groupe 29, l'expression « strictement nécessaire » implique de porter une attention particulière au principe de nécessité en raison du traitement de catégories particulières de données ainsi que de prévoir des justifications solides pour le traitement de ces données. Groupe 29, Avis 2017, p. 9.

[142] Comme pour le traitement de données à caractère personnel « non sensibles », le consentement ne devrait pas constituer une base juridique au traitement de ses données, ce traitement devant en tout état de cause être autorisée par le droit d'un État membre ou le droit de l'Union (considérant n° 37 de la directive 2016/680).

[143] Art. 10, b, de la directive 2016/680/UE.

[144] Art. 10, c, de la directive 2016/680/UE.

pour autant que l'intention de la personne soit claire[145]. Selon le Groupe 29, cette dérogation doit être interprétée de manière restrictive puisque l'inscription à un réseau social par exemple, pourrait inclure l'acceptation de règles de confidentialité (ou d'absence de confidentialité), sans que l'utilisateur n'ait pleinement conscience d'offrir par la même occasion, un accès aux informations dévoilées aux autorités répressives[146].

37. Le considérant n° 37 suggère une série de « garanties appropriées » dont la possibilité de limiter la collecte des données à celles en rapport avec la personne concernée, une sécurisation adéquate des données collectées, des conditions d'accès plus strictes et l'interdiction de transmettre ces données. Notons que le traitement de données génétiques ou biométriques nécessite de prévoir des exigences plus strictes quant à la sécurisation des données, un problème durant leur collecte pouvant mener à des faux positifs particulièrement problématiques, entres autres, dans le cadre des contrôles aux frontières[147].

38. Enfin, compte tenu des risques importants pour les droits et libertés des personnes concernées et du risque de créer des situations discriminatoires, le Groupe 29 recommande aux autorités compétentes d'effectuer une analyse d'impact préalable attestant de la nécessité du traitement. Il recommande également de prévoir des moyens matériels ou procéduraux supplémentaires tel que la soumission de l'accès aux données à l'autorisation préalable d'un organisme indépendant[148].

CHAPITRE 6. Les droits des personnes concernées

39. Afin de garantir l'effectivité des droits des personnes concernées, similairement au RGPD, la directive 2016/680/UE exige la communication des informations relatives au traitement de manière accessible, en termes clairs, simples et faciles à comprendre et ce, par tout moyen approprié, y compris par voie électronique[149] tout en tenant compte des personnes vulnérables dont les enfants[150]. Plus précisément, le responsable du trai-

[145] Groupe 29, Avis 2017, p. 10.
[146] Groupe 29, Avis 2017, p. 10.
[147] Groupe 29, Avis 06/2015, p. 8.
[148] Groupe 29, Avis 2017, p. 9.
[149] Art. 12, § 1 et considérant n° 39 de la directive 2016/680/UE ; art. 12, § 1, du RGPD.
[150] Considérant n° 39 de la directive 2016/680/UE.

tement est tenu d'informer la personne concernée de l'existence d'une opération de traitement[151], de l'identité du responsable du traitement, des finalités poursuivies, de la possibilité d'exercer un droit de réclamation et de l'existence du droit d'accès, de rectification, d'effacement ainsi que du droit de demander la limitation du traitement[152]. Ces informations peuvent figurer sur le site internet de l'autorité compétente[153] de sorte qu'il ne s'agit pas d'une obligation de notification individuelle.

40. Dans certaines circonstances particulières et pour assurer un traitement loyal des données[154], la personne est en droit d'obtenir des informations additionnelles, telles : la base juridique au traitement[155], la durée de conservation des données[156], les catégories de destinataire ou les organisations internationales[157], ou encore d'autres informations complémentaires en particulier lorsque les données sont collectées à l'insu de la personne concernée[158], par des moyens secrets ou non, par exemple, en collectant des données par vidéosurveillance ou via des proches.

41. En raison des spécificités du domaine pénal, la directive 2016/689 laisse la possibilité aux États membres de retarder ou restreindre la fourniture d'informations additionnelles, par mesures législatives, partiellement ou complètement, pour autant qu'une telle restriction soit nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne concernée, notamment en raison des besoins de l'enquête, pour sauvegarder la sécurité publique ou encore pour protéger les droits et libertés d'autrui[159]. Dès lors, dans la situation où une autorité compétente collecte des données auprès d'un acteur privé à l'insu de la personne concernée, la notification du traitement pourra être postposée pour éviter de compromettre la bonne fin de l'enquête en cours par exemple. De plus, la directive 2016/680/UE laisse la possibilité aux États membres d'adopter des mesures législatives définissant des catégories de traitement, dans leur intégralité ou en partie, pour lesquelles le droit à l'information additionnelle est exclu[160]. Ainsi, en fonction de la sensibilité de certaines bases

[151] Considérant n° 42 de la directive 2016/680/UE.
[152] Art. 13, § 1, et considérant n° 42 de la directive 2016/680/UE.
[153] Considérant n° 42 de la directive 2016/680/UE.
[154] Considérant n° 42 de la directive 2016/680/UE.
[155] Art. 13, § 2, a, de la directive 2016/680/UE.
[156] Art. 13, § 2, b, de la directive 2016/680/UE.
[157] Art. 13, § 2, c, de la directive 2016/680/UE.
[158] Art. 13, § 2, d, de la directive 2016/680/UE.
[159] Art. 13, § 3 ; 15, § 1 ; 16, § 4, et considérant n° 44 de la directive 2016/680/UE.
[160] Art. 13, § 4, de la directive 2016/680/UE.

de données, telles celles liées à la lutte contre le terrorisme, le législateur peut prévoir qu'aucune information additionnelle ne devra être fournie aux personnes concernées.

42. Concernant le droit d'accès, celui-ci doit en principe pouvoir être exercé *directement, sans frais, à intervalles raisonnables* afin de pouvoir prendre connaissance du traitement, d'en vérifier la licéité[161] mais aussi si nécessaire, d'en obtenir la rectification, l'effacement et/ou la limitation[162]. Il s'agit d'une disposition importante puisque la plupart des États membres ne prévoyaient pas d'accès direct mais se limitaient à permettre un droit d'accès indirect par le biais de l'autorité de contrôle[163]. Néanmoins, à nouveau, en raison des spécificités du domaine pénal, la directive 2016/689 laisse la possibilité aux États membres de restreindre, par mesures législatives, le droit d'accès, de rectification ou d'effacement sous réserve du respect des conditions exposées *supra*[164]. *En tout état de cause, le droit de rectification ne pourrait affecter la teneur d'une déposition*[165].

43. De plus, au lieu de procéder à l'effacement de données, la directive ouvre une nouvelle possibilité lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée mais qu'il ne peut être déterminé si ces données sont exactes ou non, ou lorsque les données à caractère personnel doivent être conservées à des fins probatoires. Il sera possible pour la personne physique de solliciter la limitation du traitement[166]. Les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer les données sélectionnées vers un autre système de traitement à des fins archivistiques, ou à rendre les données sélectionnées inaccessibles[167].

44. La restriction du droit d'accès direct ou le refus d'effacer voire de rectifier certaines données doit en principe faire l'objet d'une décision écrite et motivée[168] permettant à la personne concernée d'alors exercer son droit d'accès indirect, c'est-à-dire, de requérir l'autorité de contrôle

[161] Art. 14 de la directive 2016/680/UE.
[162] Art. 16, § 1, et considérant n° 40 de la directive 2016/680/UE.
[163] Certains États appliquaient la directive 95/46/CE par extension au régime répressif et limitait le droit d'accès aux personnes concernées conformément à l'article 13 de la directive précitée.
[164] Art. 13, § 3 ; 15 § 1 ; 16, § 4, et considérant n° 44 de la directive 2016/680/UE.
[165] Considérant n° 47 de la directive 2016/680/UE.
[166] Considérant n° 47 de la directive 2016/680/UE.
[167] Considérant n° 47 de la directive 2016/680/UE.
[168] Art. 15, § 3, 16, § 4 et considérant n° 45 de la directive 2016/680/UE.

de procéder aux vérifications et examens nécessaires[169]. La personne doit expressément être informée par cette autorité des vérifications effectuées – sans toutefois *forcément* pouvoir savoir si ses droits ont été violés – et de la possibilité de former un recours juridictionnel[170]. À nouveau, les États membres peuvent décider d'adopter des mesures législatives afin de déterminer des catégories de traitements susceptibles de relever, dans leur intégralité ou en partie, d'un quelconque des points énumérés à l'article 15, § 1, de la directive 2016/689[171] par exemple, en cas de demande d'accès à des données collectées à des fins de lutte contre le terrorisme.

45. Enfin, dans le cadre de poursuites pénales[172] ou d'une procédure judiciaire en matière pénale – que ce soit dans une décision judiciaire, un casier ou un dossier judiciaire – les droits des personnes concernées s'exercent conformément au droit interne des États membres conférant dès lors une certaine marge de manœuvre aux États membres[173].

CHAPITRE 7. Prise de décision individuelle automatisée et profilage

46. La directive 2016/680/UE interdit l'adoption de décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques « défavorables »[174] ou affectant la personne concernée de « manière significative », à moins d'être assorti de garanties appropriées et d'être autorisé par le droit de l'Union ou par le droit d'un État membre[175]. Les autorités peuvent donc, à l'instar des acteurs privés, procéder à du « datamining »[176], technique permettant, à l'aide

[169] Art. 17, § 1 de la directive 2016/680/UE.

[170] Art. 17, § 3 et considérant n° 48 de la directive 2016/680/UE. À ce propos, le Groupe 29 recommande de documenter toutes les demandes d'accès indirect, par exemple, dans un registre et d'effectuer des statistiques (Groupe 29, Avis 2017, p. 24).

[171] Art. 15, § 3, de la directive 2016/680/UE.

[172] Considérant n° 107 de la directive 2016/680/UE.

[173] Art. 18 et considérants n^{os} 49 et 107 de la directive 2016/680/UE.

[174] À la différence du RGPD, la décision ne doit pas uniquement prévoir des effets juridiques mais ceux-ci doivent être « défavorables ». Art. 22, § 1, RGDP.

[175] Art. 11 de la directive 2016/680/UE.

[176] À ce propos, voy. L. Orsi, « L'utilisation du big data pour la protection de la sécurité nationale », in *Protection des données personnelles et sécurité nationale*, Bruxelles, Bruylant, 2017, pp. 21-34.

d'algorithmes de croiser certaines données et d'anticiper des comportements ou d'établir des profils particuliers. En cas de décision automatisée, la personne concernée est en droit d'obtenir des informations spécifiques ainsi qu'une intervention humaine lui laissant la possibilité d'exprimer son point de vue et d'obtenir une explication[177].

Afin de garantir l'effectivité des droits de la personne concernée, l'homme doit être en mesure de modifier la décision et d'examiner les données pertinentes y compris celles fournies par l'intéressé[178]. On trouve une illustration de ce principe par exemple dans la directive PNR[179]. Celle-ci permet l'exploration systématique de données afin de « situer » des passagers sur une échelle de risque et d'ainsi identifier des criminels « éventuels ou probables » sans lien avec une enquête spécifique[180]. La disposition impose toutefois aux États membres de s'assurer que toute concordance positive obtenue à la suite du traitement automatisé des données des passagers fasse l'objet d'une vérification individuelle par des moyens non automatisés, afin de vérifier si des mesures effectives doivent être prises conformément au droit national[181].

47. En tout état de cause, si la directive 2016/680/UE autorise le profilage effectué sur la seule base de données sensibles *a contrario* des recommandations du Groupe 29[182] et du Conseil de l'Europe[183], elle interdit la création de profils entraînant une discrimination sur cette base[184].

---

[177] Art. 11, § 1, et considérant n° 38 de la directive 2016/680/UE.

[178] Groupe 29, Avis 2017, p. 13.

[179] Directive 2016/681/UE du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *OJ*, L 119 du 4 mai 2016, pp. 132-149 (ci-après directive PNR).

[180] Pour rappel, cette directive a été fortement critiquée par le Conseil de l'Europe (voy. en ce sens le rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, *op. cit.*). Elle a également été critiquée par le CEPD (Avis du CEPD n° 5/2015, *op. cit.*, p. 9).

[181] Art. 6, § 5, directive PNR.

[182] Le Groupe 29 recommandait pourtant d'interdire le profilage sur la seule base de données sensibles. Voy. Groupe 29, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 1er décembre 2015, p. 9.

[183] Selon le Conseil de l'Europe, la collecte et le traitement de données sensibles dans un contexte de profilage sont interdits sauf si ces données sont nécessaires et proportionnées aux finalités légitimes et spécifiques du traitement et pour autant que le droit interne prévoit des garanties appropriées. Recommandation CM/Rec (2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée le 23 novembre 2010.

[184] Art. 11, § 3, de la directive 2016/680/UE.

48. À nouveau, en raison du risque pour les droits et libertés des personnes concernées, le Groupe 29 recommande aux législateurs nationaux (et non aux autorités compétentes) d'imposer au responsable du traitement d'effectuer une analyse d'impact préalable dans les conditions prévues par l'article 27, § 1, de la directive 2016/680/UE et ainsi, d'identifier la nature des garanties spécifiques appropriées[185]. En outre, selon le Groupe 29, les lignes directrices adoptées les 3 octobre 2017[186] sont également pertinentes pour autant que l'on tienne compte des spécificités du domaines pénal[187].

CHAPITRE 8. Autorité de contrôle indépendante

49. Comme l'a rappelé la Cour de justice de l'Union européenne notamment à l'occasion de l'arrêt *Schrems*, l'institution d'une autorité de contrôle indépendante constitue un élément essentiel du respect de la protection des données[188]. En l'occurrence, les articles 41 et suivants de la directive 2016/680/UE organisent les pouvoirs de ces autorités ainsi que la coopération entre ces différentes autorités[189]. Celles-ci sont chargées de surveiller l'application des dispositions contenues dans la directive et de contrôler les opérations de traitement[190].

50. Contrairement au RGDP[191], la directive 2016/680/UE ne liste pas expressément les pouvoirs d'enquête de l'autorité de contrôle laissant aux États membres une certaine marge de manœuvre. Elle doit néanmoins disposer de pouvoirs d'enquête effectifs, et en ce sens, obtenir au minimum l'accès aux données traitées et aux informations nécessaires à l'exercice de sa mission[192]. Elle doit également disposer de pouvoirs correctifs effectifs[193] c'est-à-dire, avertir un responsable du traitement

[185] Groupe 29, Avis 2017, p. 13.
[186] Groupe 29, Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, 3 octobre 2017.
[187] Groupe 29, Avis 2017, p. 11.
[188] C.J.U.E., 6 octobre 2015, arrêt *Schrems c. Data Protection Commissionner of Ireland,* C-362/14, § 41.
[189] Art. 46 de la directive 2016/680/UE.
[190] Art. 41 de la directive 2016/680/UE.
[191] Art. 58 du RGPD.
[192] Art. 47, § 1, de la directive 2016/680/UE.
[193] Art. 47, § 2, de la directive 2016/680/UE.

d'un risque de violation des dispositions contenues dans la directive[194], ordonner de mettre dans un délai déterminé les opérations de traitement en conformité avec les dispositions contenues dans la directive[195], ou encore de limiter temporairement ou définitivement le traitement[196]. L'autorité de contrôle doit également disposer d'un pouvoir consultatif effectif c'est-à-dire, conseiller le responsable du traitement et émettre des avis[197]. Sans fixer un montant déterminé pour les amendes administratives comme le fait le RGDP[198], la directive 2016/680/UE confie aux États membres le soin de déterminer un régime de sanctions effectives, proportionnées et dissuasives et de prendre les mesures nécessaires pour garantir leur mise en œuvre[199]. En outre, chaque autorité de contrôle doit avoir le pouvoir de porter les violations des dispositions adoptées en vertu de la présente directive à la connaissance des autorités judiciaires et, le cas échéant, d'ester en justice en vue de les faire respecter[200]. Dans le même sens, toute personne concernée doit avoir le droit d'introduire un recours juridictionnel effectif contre une autorité de contrôle à l'encontre d'une décision juridiquement contraignante de cette dernière qui la concerne[201] mais aussi contre un responsable du traitement ou un sous-traitant lorsqu'elle considère que ses droits ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation desdites dispositions[202]. La personne concernée est libre de mandater un organisme, une organisation ou une association sans but lucratif agissant dans le domaine de la protection des droits et libertés pour exercer un recours en son nom[203].

51. Par ailleurs, les États membres sont libres d'instituer une autorité de contrôle compétente à la fois pour contrôler les opérations effectuées sous le volet du RGPD et de la directive[204]. Selon le Groupe 29 et le CEPD, une supervision commune devrait être encouragée afin de garantir une interprétation homogène et cohérente du régime relatif à la protection des données[205].

194 Art. 47, § 2, a, de la directive 2016/680/UE.
195 Art. 47, § 2 b, de la directive 2016/680/UE.
196 Art. 47, § 2 c, de la directive 2016/680/UE.
197 Art. 47, § 3 de la directive 2016/680/UE.
198 Art. 84 du RGPD.
199 Art. 57, § 2, a, de la directive 2016/680/UE.
200 Art. 47, § 5, de la directive 2016/680/UE.
201 Art. 53 de la directive 2016/680/UE.
202 Art. 54 de la directive 2016/680/UE.
203 Art. 55 de la directive 2016/680/UE.
204 Art. 41, § 3, de la directive 2016/680/UE.
205 Groupe 29, Avis 2017, p. 30 et CEPD, avis n° 6/2015, p. 8.

52. Enfin, en vertu de l'article 45, § 2, de la directive 2016/680, l'autorité de contrôle n'est pas compétente pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle « afin de préserver l'indépendance des juges dans l'accomplissement de leurs missions judiciaires »[206]. Selon le CEPD, cette dérogation aurait dû se limiter aux activités « purement » judiciaires à savoir, les « procès », pour limiter les risques de divergences d'interprétation eu égard aux différences importantes au sein des systèmes judiciaires des États membres. À titre illustratif, il n'est pas toujours évident de déterminer si les procureurs sont des « autorités judiciaires indépendantes »[207] ou encore, de qualifier les juridictions d'instruction. En ce sens, le considérant n° 80 précise néanmoins que la compétence de l'autorité de contrôle ne devrait pas s'étendre aux traitements de données à caractère personnel effectués par d'autres autorités judiciaires indépendantes dans l'exercice de leur fonction juridictionnelle, par exemple le ministère public[208]. En tout état de cause, le respect des règles de la présente directive par les juridictions et autres autorités judiciaires indépendantes doit toujours l'objet d'un contrôle indépendant conformément à l'article 8, § 3, de la Charte[209].

CHAPITRE 9. Transferts internationaux de données

53. La directive 2016/680/UE autorise les transferts internationaux de données par les autorités compétentes vers un pays tiers ou à une organisation internationale qualifiée d'autorité compétente[210], dans le cadre des finalités visées par l'article 1, § 1, de cette directive[211], sous réserve de l'adoption d'une décision d'adéquation adoptée par la Commission, ou en l'absence d'une telle décision, des garanties appropriées ou, en l'absence de garanties appropriée, dans le cadre des dérogations pour des situations particulières[212].

54. En l'absence de décision d'adéquation, le responsable du traitement peut autoriser le transfert de données vers un pays tiers ou à une

206 Considérant n° 80 de la directive 2016/680/UE.
207 CEPD, avis n° 6/2015, p. 8.
208 Considérant n° 80 de la directive 2016/680/UE.
209 Considérant n° 80 de la directive 2016/680/UE.
210 Art. 35, § 1, b, de la directive 2016/680/UE.
211 Art. 35, § 1, a, de la directive 2016/680/UE.
212 Art. 35, § 1, d, de la directive 2016/680/UE.

organisation internationale sous réserve de l'existence de garanties appropriées en matière de protection des données directement évaluées par ce dernier ou édictées dans un instrument juridique contraignant[213]. Le CEPD recommandait néanmoins de limiter le transfert de données à caractère personnel aux situations dans lesquelles il existe un instrument juridiquement contraignant, ou lorsqu'il est nécessaire de protéger les intérêts vitaux de la personne concernée ou dans le cas d'une menace grave et immédiate à la sécurité publique[214] et ce, conformément aux conditions exposées dans la recommandation R (87)15. En tout état de cause, ces transferts devraient être documentés et mis à la disposition de l'autorité de contrôle, sur demande, afin qu'elle puisse en vérifier la licéité[215].

Notons que selon l'article 61 de la directive 2016/680, les accords applicables avant l'entrée en vigueur de la directive demeurent inchangés. En effet, dans la mesure où antérieurement, les transferts de données entre l'UE et les pays tiers dans un contexte répressif, n'étaient pas subordonnés à l'existence d'une décision d'adéquation, des accords bilatéraux ont été conclus entre l'UE et des pays tiers. À titre illustratif, l'accord-cadre sur la protection des données signé entre les États-Unis et l'UE[216] est, selon la Commission européenne, particulièrement complet et pourrait servir de base pour négocier des accords similaires avec des pays tiers non seulement dans le domaine de la coopération judiciaire et policière, mais aussi dans d'autres domaines de l'application de la loi par les autorités publiques (par exemple, la politique de concurrence ou la protection des consommateurs)[217].

55. En l'absence de garanties appropriées constatées par le responsable du traitement, un transfert de données vers un pays tiers ou à une organisation internationale est autorisé dans un nombre limité de situations à savoir, si ce transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ; à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ; dans un cas particulier, à des fins de prévention et de détection des infractions

[213] Art. 37, § 1, a, et b, de la directive 2016/680/UE. Dans ce dernier cas, le responsable du traitement doit informer l'autorité de contrôle des catégories de transferts de données et documenter ce transfert. Art. 37, §§ 2-3.

[214] CEPD, avis n° 6/2015, p. 9.

[215] Considérant n° 72 de la directive 2016/680/UE.

[216] Accord, entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, *J.O.*, L 336 du 10 décembre 2016, pp. 3-13)

[217] Communication de la Commission au Parlement et au Conseil, « Échange *et* protection *de* données *à* caractère personnel *à l'*ère *de la* mondialisation », COM(2017) 7,10 janvier 2017, p. 16.

pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; ou, dans un cas particulier, à la constatation, l'exercice ou la défense de droits en justice[218]. Par ailleurs, le considérant n° 72 précise que « ces dérogations devraient être interprétées de manière restrictive et ne devraient pas permettre des transferts fréquents, massifs et structurels de données à caractère personnel ni des transferts de données à grande échelle, mais des transferts qui devraient être limités aux données strictement nécessaires ».

56. De plus, lorsque des données proviennent *d'un autre* État membre et sont transférées ultérieurement vers un autre pays tiers ou à une autre organisation internationale, l'État membre ayant traité les données initialement doit, en règle générale, donner son consentement avant le transfert conformément à son droit national[219]. À cette fin, l'État en question est tenu de prendre en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement[220]. Par exception, une autorisation ne doit pas être requise dans la situation où ce transfert est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile[221]. L'État membre ayant traité les données initialement doit cependant en être informé sans retard[222].

57. En outre, si en principe la coopération policière et judiciaire s'exerce entre les autorités compétentes, le droit de l'Union ou le droit d'un État membre peut, dans certains cas particuliers, autoriser le transfert de données à caractère personnel directement vers d'autres types de destinataires établis dans des pays tiers. Ce transfert suppose le respect de conditions cumulatives justifiant la proportionnalité et la nécessité du transfert à ce destinataire et non à l'autorité compétente[223]. Cette situation pourrait se

[218] Art. 36 de la directive 2016/680/UE.
[219] Art. 35, § 1, c, de la directive 2016/680/UE.
[220] Art. 35, § 1, e, de la directive 2016/680/UE.
[221] Art. 35, § 2, de la directive 2016/680/UE.
[222] Art. 35, § 2, de la directive 2016/680/UE.
[223] Ainsi, l'article 39, § 1, de la directive 2016/680/UE précise un ensemble de conditions à savoir : le transfert est strictement nécessaire à l'exécution de la mission de l'autorité

présenter en cas d'attentat terroriste imminent, lorsque l'autorité compétente cherche à obtenir en urgence l'identité du titulaire d'un compte bancaire auprès d'une banque située hors du territoire de l'Union européenne afin d'identifier les suspects dans le cadre de cette enquête pénale. Enfin, l'article 39, § 1, de la directive 2016/680/UE impose de tenir compte des accords internationaux conclus afin de vérifier si ce transfert de données vers des entités privés n'a pas été expressément exclu lors de la conclusion de cet accord.

Conclusions

58. Alors que la décision-cadre 2008/977 limitait son champ d'application aux flux transfrontières de données, la directive 2016/680/UE s'applique aux traitements de données effectués sur le territoire interne des États membres et au-delà. Plus qu'un cadre visant à favoriser l'échange de données à des fins de coopération policière et judiciaire, elle offre une base commune de protection des données dans un contexte répressif tout en cherchant à ménager un équilibre entre le besoin de garantir la sécurité publique et la nécessité de protéger le droit à la protection des données à caractère personnel. À titre illustratif, elle généralise le droit d'accès direct tout en organisant un panel d'exceptions permettant de limiter, partiellement ou totalement, ce droit pour diverses raisons telles que les nécessités de l'enquête.

59. Malgré des différences importantes au sein des systèmes judiciaires des États membre, la directive 2016/680/UE se donne pour objectif ambitieux de légiférer dans le domaine de la « police » et de la « justice », domaine traditionnellement considéré comme relevant de leur souveraineté nationale. On peut cependant s'inquiéter du fait que certaines notions n'aient pas été davantage précisées entraînant un risque

compétente qui transfère les données ainsi que le prévoit le droit de l'Union ou le droit d'un État membre aux fins énoncées à l'article 1er, § 1 ; l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question ; l'autorité compétente qui transfère les données estime que le transfert à une autorité qui est compétente aux fins visées à l'article 1er, paragraphe 1, dans le pays tiers est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun et informe dans les meilleurs délais cette dernière de ce transfert ; l'autorité compétente effectuant le transfert informe également le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire.

d'aboutir à des niveaux de protection des données distincts selon les États membres, par exemple lorsqu'il s'agit de déterminer les traitements de données effectuées à des fins de « prévention de la menace ». De plus, compte tenu de l'importance de l'autorité de contrôle dans le domaine de la protection des données, on peut regretter que les pouvoirs de sanctions « effectifs » de cette autorité n'aient pas davantage été précisés. De même, il est étonnant que le ministère public soit expressément exclu de son pouvoir d'examen, à l'instar des cours et tribunaux dans le cadre de leurs fonctions juridictionnelles et ce, peu importe son statut en droit interne.

60. On peut en revanche saluer, la mise sur pied d'un cadre général relatif aux transferts internationaux de données vers des pays tiers et ce, même s'il présente une souplesse certaine ouvrant la voie à un risque de connaître un amenuisement des règles relatives à la protection des données. On peut également saluer la cohérence de la directive 2016/680/UE vis-à-vis du RGDP compte tenu de l'intensification des échanges entre les entités privées et les autorités répressives voire du rôle de plus en plus étendu que les autorités répressives leur accorde dans la collecte de preuves. Toutefois, une faiblesse majeure inhérente à l'adoption d'un instrument spécifique dans le domaine de la protection des données est celle d'aboutir à une restriction des garanties offertes aux personnes concernées en raison des besoins de la « police » et de la « justice ».