Lutte contre le terrorisme et protection effective des données à caractère personnel : une conciliation délicate

Vincent BOUHIER
Maître de conférences HDR en droit public, Université d'Evry-Val d'Essonne, Université de Paris-Saclay
Centre de recherche Léon Duguit (EA4107)

Résumé : *La protection des données à caractère personnel est inégalement abordée par le droit de l'Union européenne au moment de l'élaboration des normes ayant pour objet direct ou indirect de lutter contre le terrorisme. L'appréhension demeure très abstraite pour les dispositions internes, la Commission et le Conseil privilégiant les impératifs de sécurité. En revanche, sous l'influence déterminante du Parlement européen, les accords internationaux envisagent plus concrètement la protection de ce droit. Si à l'avenir un renforcement de la protection peut être espéré, lors de l'élaboration de toutes les dispositions de l'Union, avec l'intervention plus systématique du Parlement, cet effort restera insuffisant sans l'insertion de mécanismes de contrôle appropriés, une fois les textes entrés en vigueur. Aujourd'hui, seul le contrôle des actes de portée générale par la Cour de justice de l'Union européenne apparaît effectif.*

1. La multiplication des actes de l'Union européenne consacrés directement ou indirectement au terrorisme démontre que la lutte contre le terrorisme n'a pas seulement une dimension étatique, mais également une dimension européenne et même internationale[1]. Il est vrai que le terrorisme s'affranchit des frontières tant dans sa préparation que dans ses actes. Les terroristes usent pleinement des capacités de mobilité qu'offre l'Union européenne et notamment l'espace Schengen, au sein duquel le contrôle systématique aux frontières a été aboli pour les États y participant[2].

2. Dans cette perspective, il est apparu opportun aux États membres de confier certaines de leurs compétences à l'Union, dans le cadre de la coopération policière et judiciaire, afin de lutter plus efficacement contre le terrorisme, l'approche nationale s'avérant insuffisante[3]. Il s'agit aujourd'hui de faire face à un terrorisme plus diffus, plus difficilement décelable, en raison des moyens de communication utilisés, et reposant davantage sur des passages à l'acte individuel, qui exige de recueillir de nombreuses informations au moins à des fins de prévention. L'exigence de résultats a nécessité tout d'abord de retenir une définition commune, posée dans la décision-cadre du 13 juin 2002[4] et modifiée en 2008 pour élargir le contenu, impliquant de mieux contrôler internet pour identifier les hypothèses de provocation

[1] Conseil de l'Union européenne, Stratégie de l'Union européenne visant à lutter contre le terrorisme, Bruxelles, 30 nov. 2005, 14469/4/05/REV 4, p. 7.
[2] Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO L 239, 22 sept. 2000, p. 19
[3] Cons ; 9, de la décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, JOCE L 164, 22 juin 2002, p.4.
[4] *Idem*, art. 1, § 1, p. 4.

publique à commettre une infraction terroriste[5]. Ensuite, l'Union a été le support de stratégie, de programme[6] intégrant la création de nouveaux instruments ou l'interconnexion d'instruments préexistants au niveau national, principalement en matière de collecte et d'analyse d'informations.

3. La lutte contre le terrorisme à l'échelle de l'Union n'est pas nouvelle, elle s'est simplement amplifiée au fur et à mesure que d'importants actes terroristes se déroulaient dans les États occidentaux. Les premiers textes relatifs à la question du terrorisme ont été adoptés dans le courant des années quatre-vingt-dix. Cependant l'adoption d'actes contraignants va réellement débuter après les attentats du 11 septembre 2001, connaissant une croissance constante en raison de l'insertion de fondements juridiques tant dans le Traité de Nice que dans le Traité de Lisbonne[7]. Au-delà des actes contraignants, de nombreuses communications ont été adoptées par la Commission à la suite de conclusions du Conseil européen, exigeant de renforcer l'arsenal en matière de lutte contre le terrorisme. Si des textes visent directement et exclusivement la lutte contre le terrorisme, d'autres textes ne l'abordent qu'indirectement, parmi les objectifs pouvant être dévolus à la proposition initiale[8]. Les textes sont en conséquence multiples, de nature et de contenus très différents, rendant difficile une appréhension exhaustive du terrorisme par l'Union européenne.

4. Les échanges d'information constituent un axe essentiel de la lutte contre le terrorisme dans l'Union européenne. En se référant à sa stratégie visant à lutter contre le terrorisme[9], il est possible de constater que l'accès et l'échange d'informations irriguent les facettes de cette lutte. En effet si l'Union a défini une stratégie se décomposant en quatre domaines d'action, la prévention, la protection, la poursuite et la réaction[10], il est nécessaire à chaque fois de recourir à l'échange d'informations entre services des États membres, mais également parfois avec les Etats tiers. C'est ainsi que les institutions n'ont pas toujours été à l'origine des textes, les États membres ayant parfois anticipé les moyens d'actions par des traités bilatéraux qui ont été ensuite repris par l'Union[11]. Cette voie a permis de répondre plus rapidement aux exigences de sécurité, sans passer par les méandres des procédures de l'Union[12]. Si elle

---

[5] Article 3 de la décision-cadre 2008/919/JAI du Conseil du 28 nov. 2008 modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme, JOUE L 330, 9 déc. 2008, p. 21.

[6] Notamment la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Le programme européen en matière de sécurité, Strasbourg, 28 avr. 2015, COM(2015) 185 final, p.1-24.

[7] Sur ce point, v. Josiane Auvret-Finck, « Le cadre juridique de référence de la lutte contre le terrorisme », *in* J.Auvret-Finck (dir.), *L'Union européenne et la lutte contre le terrorisme. Etat des lieux et perspective*, Larcier, Bruxelles, 2010, p.17 et s.

[8] Dir. 2006/24/CE du Parlement et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la dir. 2002/58/CE, JOUE L 105, 13 avr. 2006, p. 54.

[9] Conseil de l'Union européenne, *Stratégie de l'Union européenne visant à lutter contre le terrorisme*, Bruxelles, 30 nov. 2005, 14469/4/05/REV 4, p. 1-45

[10] *Idem*, p. 3

[11] C'est le cas notamment du Traité de Prüm, signé le 27 mai 2005, dont l'objet était d'approfondir la coopération transfrontalière entre les autorités policières et judiciaires des pays de l'Union notamment par la création de fichiers nationaux d'ADN. Ce traité a ensuite été intégré dans l'ordre juridique de l'Union par une décision du Conseil. Décision du Conseil 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JOUE L 210, 6 août 2008, p. 1.

[12] Sophie Perez et Thierry Thibaud, « Les instruments de lutte contre le terrorisme au sein de l'Union européenne », dans J.Auvret-Finck (dir.), *L'Union européenne et la lutte contre le terrorisme. Etat des lieux et perspective*, *op. cit.*, p. 98.

concentre la plupart de ses actes sur les informations domestiques[13], c'est-à-dire celles détenues par les États membres ou les organismes de l'Union, des accords avec les pays tiers ont également été négociés et adoptés parfois dans la douleur. C'est le cas de l'accord SWIFT[14] et des accords PNR (*Passengername record*)[15].

5. La volonté de lutter efficacement contre le terrorisme s'accompagne au sein de l'Union européenne d'une autre préoccupation, celle du respect des droits fondamentaux. Cette exigence est affirmée dès la décision-cadre de 2002[16]. Ainsi, la lutte contre le terrorisme ne situe pas en marge des autres domaines d'intervention de l'Union. Il y a une soumission pleine et entière à l'article 2 du Traité sur l'Union européenne, précisant qu'elle « est fondée sur les valeurs de respect, de dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit ainsi que de respect des droits de l'Homme, y compris des droits des personnes appartenant à des minorités ». La Charte des droits fondamentaux de l'Union a concrétisé plus largement cet attachement, en devenant contraignant conformément à l'article 6, paragraphe 1 TUE issu du Traité de Lisbonne. Toutefois, l'articulation entre le respect des droits fondamentaux et la lutte contre le terrorisme n'apparaît pas toujours avec évidence. Il existe une tension entre la protection des libertés individuelles et les impératifs sécuritaires[17]. Les exigences de transparence, de contrôle démocratique, plus largement le principe de l'Etat de droit, ne s'affirment pas toujours comme des préoccupations prioritaires, l'efficacité étant privilégiée. Or toute contrainte posée à la collecte et à l'accès à l'information est conçue comme contreproductive et source d'impuissance. A cet égard, la Cour de justice a déjà dû à plusieurs reprises s'employer pour imposer le respect de certains droits. L'arrêt Kadi[18] est sans doute le contentieux le plus emblématique, mais d'autres affaires méritent tout autant une attention parce qu'elles ont mis l'accent sur d'autres droits plus fragiles, dont le droit à la protection des données à caractère personnel[19]. Il est vrai que les droits de la défense focalisent souvent l'attention en matière de droits fondamentaux, étant donné que le terrorisme conduit à des régimes d'exception[20]. Le droit à la protection des données à caractère personnel entre ainsi en contradiction avec la collecte, l'échange d'informations, la constitution de fichiers ou encore la surveillance des données générées par les communications électroniques nécessaires à la lutte contre le terrorisme mais également contre d'autres comportements criminels. Au regard de la volonté affichée par l'Union en matière de respect des droits fondamentaux, ce droit devrait être effectivement protégé. Les

[13] Par exemple, la décision2005/671/JAI du Conseil du 20 sept. 2005 relative à l'échange d'informations et à la coopération concernant les infractions de terrorisme, JOUE L 253, 29 sept. 2005, p.22.

[14] Décision 2010/412/UE du Conseil du 13 juil. 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JOUE L 195, 27 juil. 2010, p. 3.

[15] Décision 2012/472/UE du Conseil du 26 avr. 2012 relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure JOUE L 215 du 11 août 2012, p. 4. Marie-Françoise Labouz, « Le nouvel accord sur les données de passagers aériens (PNR) entre l'Union européenne et les Etats-Unis », in Emmanuelle Saulnier-Cassia, *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne »*, LGDJ, Paris, 2014, pp. 265-275.

[16] Article 1, § 2 de la décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, préc., p. 4.

[17] En ce sens Maurice Weyembergh, « Le terrorisme et les droits fondamentaux de la personne. Le problème », in Emmanuelle Bribosia et Anne Weyembergh (dir.), *Lutte contre le terrorisme et droits fondamentaux, droit et justice*, Bruylant, Bruxelles, 2002, pp. 11-35.

[18] CJCE, 3 sept.2008,*Kadi al Barakaat*, aff.Jointes C-402/05 P et C-415/05 P, ECLI:EU:C:2008:461.

[19] CJUE, 8 avr. 2014, *Digital Rights Ireland Ltd c.Minister for communication, Marine and Natural ressources et autres, KärntnerLandesregierung*, C-293/12 et C-594/12, ECLI:EU:C:2014:238.

[20] CJUE, 4 juin 2013, *ZZ c. Secretary of State for the Home Department*, C-300/11, ECLI:EU:C:2013:363; CJCE, 3 sept.2008,*Kadi al Barakaat*, précité.

différents textes adoptés par l'Union reprennent d'ailleurs cette exigence de respect des droits fondamentaux, sans toujours viser le droit à la protection des données à caractère personnel. Malgré cette omission, cette protection est une préoccupation constante, voire omniprésente, au stade de l'élaboration de toutes les dispositions visant à l'échange d'information (I). Néanmoins, une fois ces dispositions adoptées et entrées en vigueur, la protection effective de ce droit est partielle (II).

I. Une protection des données à caractère personnel recherchée au moment de l'élaboration de la norme

6. La protection des données à caractère personnel transparaît au moment de l'élaboration de la norme, mais de manière relativement abstraite dans les normes destinées uniquement à un usage au sein de l'Union européenne (A). En revanche, la pression est nettement plus prononcée pour le respect de ce droit dans les accords internationaux sous l'impulsion du Parlement européen (B).

A) Une appréhension abstraite de la protection des données à caractère personnel dans les normes internes à l'Union

7. L'examen des différents textes, qu'ils visent directement ou non à lutter contre le terrorisme, démontre que les droits fondamentaux sont envisagés dès lors qu'il est question de collecte, de stockage, d'établissement de fichiers ou d'échanges d'informations. Ce souci est intégré dans tous les textes qu'ils soient ou non contraignants[21]. Il s'agit d'une exigence récurrente, écartant toute idée d'un régime d'exception. Les droits fondamentaux sont présentés comme constituant un fondement de la politique de sécurité[22]. Des précautions sont même prises pour affirmer cet équilibre. C'est ainsi que la décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme précise que « *rien dans la présente décision-cadre ne peut être interprété comme visant à réduire ou à entraver des droits ou libertés fondamentales telles que le droit de grève, la liberté de réunion, d'association, ou d'expression…* »[23].

8. La référence à la question des droits fondamentaux est abordée de manière générale dans les considérants des actes contraignants de l'Union en lien avec la lutte contre le terrorisme[24]. Cependant une référence plus précise à certains droits peut être effectuée, notamment « *au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel* »[25]. La présence de considérants, pour rassurante qu'elle puisse être, n'est pas satisfaisante puisqu'ils sont en réalité isolés. Il n'existe pas disposition contraignante pendante précisant les conditions permettant de garantir concrètement ce droit, ne serait-ce que sous la forme d'un droit de rectification ou d'effacement. Il y a une ambiguïté sur la portée de cette protection qui s'avère en réalité uniquement abstraite, en l'absence de réelles prescriptions.

---

[21] Rapport annuel de l'UE sur les droits de l'homme 2008, 14146/2/08REV 2, 27 nov. 2008, p. 80.

[22] Communication de la Commission au Parlement et au Conseil, Stratégie de sécurité intérieure de l'UE en action : cinq étapes vers une Europe plus sûre, 22 nov. 2010, COM (2010) 673 final, p.3.

[23] Considérant 10 de la décision-cadre du 13 juin 2002, préc.

[24] Cons. 22 de la dir. 2006/24, préc.et cons. 7 de la décision 2005/671/JAI du Conseil du 20 sept. 2005 relative à l'échange d'informations et à la coopération concernant les infractions terroristes, JOUE L 253, 29 sept. 2005, p. 22.

[25] Cons. 22, dir. 2006/24, préc.

9. Ce droit est confronté à la logique de fond des institutions comme des États membres qui visent prioritairement à établir une politique de sécurité publique et de sûreté de l'Etat plus efficace. L'ensemble des dispositions est consacré à garantir un meilleur accès en masse et en temps réels. La protection des données est très largement accessoire. Ceci est renforcé par le contenu même des textes de l'Union qui ne sont que peu précis sur les données devant être conservées ? Par qui peuvent-elles être consultées ? Dans quelles conditions peuvent-elles être consultées ? De même si des organes de contrôle sont créés, ils ont pour mission de vérifier la bonne application des dispositions par les autorités, sans pour autant pouvoir être saisis par les citoyens contre d'éventuels abus.

10. Cette atteinte est aujourd'hui potentiellement de grande ampleur au regard de la multiplication des fichiers existants auxquels de nombreuses autorités peuvent avoir accès[26]. Parmi les fichiers les plus importants, il y a le Système d'information Schengen, deuxième génération (SIS II), qui est un instrument de partage d'informations accessibles aux autorités nationales, alimenté par ces mêmes autorités et Interpol, sans véritable contrôle sur le bien-fondé de l'inscription[27]. S'ajoute le fichier instauré par le Traité de Prüm, qui concerne la comparaison automatisée d'ADN[28], mais également le système européen d'information sur les casiers judiciaires (ECRIS), le système d'index européen des registres de la police (EPRIS), l'environnement commun de partage de l'information en matière maritime (CISE). Il doit également être fait état de la base de données européenne sur les bombes (EBDS), du système d'information Europol (SIE), qui peut faire l'objet d'échanges de données avec d'autres fichiers d'analyse (IS)[29] et du fichier sur les visas de courte durée (VIS)[30]. Il s'agit là d'une partie seulement des fichiers existants. Cette multiplication des supports juridiques traduit une approche sécuritaire, tout à fait légitime. Toutefois, l'éclatement des données, alimentées et consultées au regard de règles souvent distinctes, gérées par des personnes publiques différentes, ne permet pas d'appréhender la protection des données autrement que de manière très générale.

11. Il convient de préciser qu'une évolution se dessine au regard d'une communication de la Commission sur le programme européen en matière de sécurité datant du 28 avril 2015[31]. La Commission a en effet rappelé qu'il fallait veiller au respect absolu des droits fondamentaux, l'apparition du terme "absolu" est la marque d'une exigence plus élevée, exprimant également que le respect n'était sans doute pas suffisant jusque-là. La Commission insiste plus particulièrement sur la protection des données personnelles en précisant que *« l'incidence de toute nouvelle initiative sur la libre circulation et la protection des données à*

[26] Communication de la Commission au Parlement et au Conseil, Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, Bruxelles, 20 juil. 2010, COM(2010) 385 final, 67 p.

[27] Règlement (CE) n°1987/2006 du Parlement et du Conseil du 20 déc. 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JOUE L 381, 28 déc. 2006, p. 4.

[28] Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JOUE L 210, 6 août2008, p. 1 et décision 2008/616/JAI du 23 juin 2008relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JOUE L 210, 6 août2008, p. 12.

[29] Décision-cadre 2008/977/JAI du Conseil du 27 nov. 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JOUE L 350, 30 déc. 2008, p. 50

[30]Régl.n°767/2008 du Parlement et du Conseil du 9 juil. 2008 concernant le système d'information sur les visas, JOUE L 218, 13 août 2008, p. 60.

[31] Communication de la Commission, Le programme européen en matière de sécurité, préc.

caractère personnel doit être parfaitement conforme au principe de proportionnalité et aux droits fondamentaux »[32]. Cette conversion de la Commission se fait sous l'influence de la Cour de justice, mais elle est intéressante en ce qu'elle oblige à intégrer des éléments de régulation et de contrôle pour accéder aux données au sein même des dispositions européennes et à ne pas renvoyer aux États membres le soin de décider du degré de protection. Cette ambition de la Commission correspond aux exigences en vigueur dans les échanges d'informations avec les pays tiers, lorsqu'un accord est adopté.

B) Une appréhension concrète de la protection des données à caractère personnel dans les accords internationaux

12. La lutte contre le terrorisme passe également par la conclusion d'accords internationaux, notamment afin de pouvoir échanger des informations, étant donné que les terroristes font fi des frontières. Les États-Unis sont notamment particulièrement demandeurs d'accès à des informations pouvant être collectées au sein de l'Union européenne, mais ce ne sont pas les seuls, le Canada[33] ou l'Australie[34] pouvant être également cités. La logique aurait voulu que de tels accords soient adoptés sans grande difficulté, les institutions et les Etats membres ayant progressivement fait le choix en faveur de la collecte, du stockage et d'un accès toujours plus conséquent aux informations.

13. Ce n'est pas la situation qui a prévalu, l'adoption de tels accords ayant été freinée par le Parlement européen. Depuis le Traité de Lisbonne, l'article 218, paragraphe 6, point a) TFUE attribue davantage de pouvoirs au Parlement européen dans le domaine des relations extérieures de l'Union, en insérant une procédure d'avis conforme, chaque fois qu'un accord intervient dans un domaine où la procédure législative ordinaire s'applique. En conséquence, le Parlement dispose de la faculté de rejeter la conclusion d'un accord. C'est notamment l'hypothèse de l'article 87, paragraphe 2 qui vise l'adoption de mesures sur la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes. Cette situation s'est produite le 11 février 2010 à l'égard de la proposition de la décision du Conseil relative à la conclusion d'un accord intérimaire entre l'Union européenne et les Etats-Unis sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux fins du programme de surveillance du financement du terrorisme[35] (dit accord SWIFT[36]). Cet accord venait en réalité légaliser une pratique en cours depuis 2001, les Etats-Unis exploitant secrètement les données bancaires. Pour le Parlement européen, l'accord posait des difficultés en raison du volume de données à transmettre, sans que celles-ci puissent être corrigées ultérieurement par des mécanismes de surveillance ou de contrôle. En outre, le transfert des données n'était pas limité dans le temps et ne nécessitait pas l'intervention d'une autorité judiciaire. Enfin, l'accord ne limitait pas clairement le transfert aux seuls Etats-Unis, cet Etat pouvant éventuellement transmettre les données à des pays tiers. Selon le Parlement, cet accord ne garantissait pas « *aux citoyens européens et aux entreprises européennes les mêmes*

[32] *Idem*, p. 3

[33] Résolution du Parlement européen du 5 mai 2010 sur le lancement des négociations sur les accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada, JOUE C 81[E],15 mars 2011, p. 70.

[34] Décision 2012/381/UE du Conseil du 13 déc. 2011 relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, JOUE L 186, 14 juil. 2012, p. 3.

[35] Résolution législative P7_TA-PROV(2010)0029.

[36] SWIFT signifie *Society for Worldwide Interbank Financial Telecommunication* ; il s'agit du nom d'une société domiciliée en Belgique dont l'objet social est de gérer un réseau de données bancaires.

droits et garanties au titre de la législation américaine que ceux dont ils bénéficieraient sur le territoire de l'UE »[37].

14. Face à cette position ferme et nécessairement insurmontable en raison de l'avis conforme, les institutions européennes ont été obligées de négocier un nouvel accord, nécessitant de prendre en considération concrètement la problématique de la protection des données à caractère personnel. Il a ainsi été introduit plusieurs dispositions afin de remédier aux insuffisances du texte initial, notamment en faisant d'Europol un organe de contrôle des demandes émanant du Trésor américain, en limitant l'usage des données transmises au cas de terrorisme ou encore en précisant les conditions de stockage, la durée de conservation et en interdisant l'interconnexion avec d'autres fichiers. De plus il a été inséré à l'égard de toute personne la capacité de pouvoir saisir les autorités américaines afin de connaitre le contenu des données transférées le concernant (art. 15). Au-delà de la question de l'effectivité liée à la mise en œuvre de ces dispositions, il apparait que l'accord international est finalement plus complet que les actes adoptés en interne. La protection n'est plus seulement un objectif énoncé, elle trouve une traduction identifiable au sein de dispositions contraignantes de l'accord. C'est d'ailleurs ce qui a justifié que le Parlement européen se prononce en faveur de la conclusion de l'accord renégocié, entrée en vigueur le 1er août 2010.

15. Les différents accords sur le transfert des données des passagers au pays tiers ont connu un cheminement presque équivalent, le Parlement européen se montrant hostile, sachant qu'il n'était pas consulté avant l'entrée en vigueur du traité de Lisbonne. La voie juridictionnelle a dès lors été privilégiée, conduisant, par un arrêt de la Cour[38], à l'annulation du premier accord PNR UE-Etats-Unis[39]. Le Parlement européen a également saisi la Cour de justice d'une demande d'avis, le 10 avril 2015 sur le fondement de l'article 218, paragraphe 11 TFUE[40], démontrant à nouveau son scepticisme sur la compatibilité du contenu de l'accord, l'angle étant toujours la violation de la protection des données à caractère personnel. Cette opposition n'est que temporaire. Elle est levée si les préoccupations du Parlement sont intégrées à l'accord renégocié. Ainsi le Parlement a donné son accord, le 19 avril 2012[41], à la conclusion de l'accord PNR UE-Etats-Unis, à l'égal de l'accord SWIFT, les garanties intégrées étant, cette fois, substantielles.

16. Le Parlement européen joue en conséquence un rôle essentiel, depuis le traité de Lisbonne, en matière d'accords internationaux. Une approche similaire devrait être constatée pour les textes internes à l'Union européenne. Le traité de Lisbonne a, en effet, également renforcé les pouvoirs du Parlement dans le cadre de l'espace de justice, de liberté et de sécurité. Ainsi, il est précisé à l'article 87, paragraphe 2,visant tous les aspects de la coopération policière relevant des atteintes à la protection des données personnelles, que l'adoption des textes se fait par un recours à la procédure législative, alors que sous le traité de Nice, seul le Conseil intervenait conformément à l'article 34, paragraphe 2 TUE en vigueur à l'époque. Le Parlement européen peut en conséquence s'affirmer comme le gardien des droits fondamentaux, étant en mesure d'exiger de plus amples garanties en tant que colégislateur. C'est ce qui s'est produit concernant le PNR européen, voulu par la Commission et le Conseil. Une proposition de directive avait été déposée en 2011, rejetée

[37] Recommandation du 5 fév. 2010, Rapporteure Jeannine Hennis-Plasschaert, A7-0013/2010, p. 9.
[38] CJCE, 30 mai 2006, *Parlement européen c. Conseil*, C-317/04 et C-318/04, ECLI:EU:C:2006:346.
[39] Décision 2004/496/CE du Conseil, du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure.
[40] CJUE, avis 1/15, JOUE C 138, 27 avr. 2015 p. 24.
[41] Parlement européen, 19 avr. 2012, P7_TA(2012)0134

fermement par le Parlement européen le 24 avril 2013. Fort de garanties supplémentaires sur la protection des données personnelles, notamment avec la révision de la directive de base sur la protection des données personnelles[42], le Parlement a donné son accord de principe pour la directive le 9 juillet 2015[43].Ainsi le rapport de force modifie progressivement et sans doute durablement l'équilibre au moment de l'élaboration des textes. Il n'en reste pas moins que cette évolution ne saurait être suffisante si une protection effective n'existait pas une fois les dispositions entrées en vigueur.

II. Une protection des données à caractère personnel effective partielle après l'entrée en vigueur

17. Les données personnelles sont collectées le plus souvent sans que la personne concernée en ait pleinement connaissance, voire à son insu, ou sans même qu'elle sache que les données sont consultées et analysées. S'il existe des mécanismes de contrôle, ceux-ci apparaissent inappropriés (A), seule la voie juridictionnelle apparait efficace lorsqu'elle porte sur la contestation directe de l'acte de portée générale (B).

A Des mécanismes de contrôle inappropriés

18. La difficulté en matière de protection des données à caractère personnel est de faire face à la multiplicité des instruments de gestion de l'information. Cet éclatement des instruments empêche un véritable contrôle effectif étant donné que les instruments ne fonctionnent pas de manière identique et ne prévoient pas de mécanismes d'accès à l'information détenue pour obtenir une rectification ou un effacement.

19. Cette diversité des instruments se perçoit d'abord au niveau de la collecte de l'information. Seuls certains instruments prévoient une collecte ou un stockage de données à caractère personnel au niveau de l'Union. Parmi ces instruments, peuvent être cités le Système d'information Schengen II, Europol, Eurojust ou encore le Système d'information sur les visas (VIS). Tous les autres instruments relèvent de système d'échanges décentralisés, les données étant collectées au niveau national par les pouvoirs publics ou des entreprises privées. L'Union européenne intervient dans cette dernière hypothèse pour faciliter l'échange d'informations. Ensuite certains instruments sont interconnectés alors que d'autres sont isolés. En conséquence, des informations peuvent être collectées à plusieurs reprises pour des instruments différents, indépendamment de l'existence d'une interconnexion. C'est le cas, par exemple, de données biographiques qui se retrouvent dans différents fichiers ou encore des données biométriques. En revanche, certaines données peuvent uniquement relevées d'un système, tels que les profils ADN, mais ensuite être transmises vers Europol ou Eurojust.

20. Ces collectes d'informations ont des incidences directes, puisque, dans certains cas, elles peuvent aboutir à l'absence de délivrance d'un visa. C'est l'objet principal du Système d'information Schengen[44]. Elles peuvent également nourrir une enquête. C'est ainsi qu'il est expressément prévu dans la décision du 20 septembre 2005 relative à l'échange d'information et à la coopération concernant les infractions terroristes que « *toute information pertinente contenue dans un document, dossier, élément d'information, objet ou autre moyen de preuve,*

[42]Dir. 95/46/CE du Parlement et du Conseil du 24 oct. 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, JOUE L 281, 23 nov. 1995, p. 31.
[43] Point 27 de la résolution, P8_TA-PROV(2015)0269, p. 8.
[44] Art. 2 du Règl. (CE) n°1987/2006 du Parlement et du Conseil du 20 déc. 2006, préc., p. 7.

qui a été saisi ou confisqué au cours d'une enquête ou de procédures pénales en rapport avec des infractions terroristes, puisse être accessible dès que possible aux autorités d'autres Etats membres intéressés conformément au droit national »[45]. Il faut préciser que le droit national est nécessairement influencé par les obligations issues du droit de l'Union. Ainsi, des informations sur une personne, alors même qu'aucune condamnation n'a été prononcée, peuvent circuler sans que l'individu puisse s'y opposer, auprès des autorités concernées, et surtout sans qu'il puisse demander des rectifications, postérieurement, auprès de ces mêmes autorités. L'absence de connaissance de la diffusion de l'information rend tout contrôle purement théorique. Très peu de données sont transmises volontairement par les personnes, à l'exemple du transfert des données des dossiers de passagers aux pays tiers (PNR). Ce fichier constitue sans doute le moins méconnu des personnes physiques étant donné que ce sont elles qui fournissent directement les renseignements collectés. Cependant une partie des données est directement issue du passeport sans que la personne en soit clairement avertie. Ainsi même dans l'hypothèse d'une connaissance de la transmission de l'information, le cheminement suivi par les données est complexe et rend compliqué en soi, l'éventuel droit d'accès que souhaiterait obtenir un citoyen. En outre, ce n'est pas parce qu'une information est modifiée dans une base de données qu'elle le sera nécessairement dans les autres. Il n'existe pas de droit général au déréférencement, seul le temps peut faire son œuvre au regard des délais de conservation.

21. Cependant, la connaissance de la transmission de données a une incidence. Dans le cadre des accords PNR, il est prévu expressément un droit d'accès avec une procédure qui est précisée à l'article 15 pour l'accord PNR UE-Etats-Unis et un droit de rectification, d'effacement ou de verrouillage (article 16). Les dispositions peuvent apparaitre limitées, elles ont au moins le mérite d'exister puisqu'il peut être opéré un contrôle à l'initiative de l'individu concerné. Seul l'individu apparait à même de défendre son droit à la protection des données à caractère personnel. En effet, les institutions chargées de protéger les droits des citoyens européens ne le font pas nécessairement. La mise en œuvre de l'accord SWIFT a posé de sérieuses difficultés, la NSA ayant transféré une partie des données financières personnelles au mépris du contenu de l'accord. Seul le Parlement européen a réagi demandant à la Commission de suspendre l'accord, ce qui n'a pas été réalisé. Il faut préciser parallèlement que, s'il existe un contrôleur européen de protection des données, celui-ci apparait bien insuffisant pour offrir une protection effective dans le domaine des données en lien avec le terrorisme, n'ayant pas de pouvoir contraignant ou coercitif face aux différents organes de l'Union et aux Etats membres.

22. Dans ces conditions le contrôle apparait bien faible qu'il soit *a priori,* par les institutions ou même les individus au moment où l'information va être collectée, ou qu'il soit *a posteriori,* l'individu n'ayant pas connaissance ou pas conscience de l'utilisation des données le concernant.

B) Le contrôle juridictionnel effectif des actes de portée générale

23. L'accès au juge est une donnée essentielle pour la protection des droits fondamentaux. Concernant la protection des données à caractère personnel, le juge national est généralement compétent étant donné que les décisions faisant grief sont prises au niveau des Etats membres à partir des instruments décidés au niveau de l'Union. Ainsi, lorsque le Système d'information Schengen est utilisé à l'égard d'un individu, c'est un Etat qui décide de refuser l'entrée sur

[45] Art. 2, par. 6 de la décision 2005/671/JAI du Conseil du 20 sept. 2005 relative à l'échange d'informations et à la coopération concernant les infractions terroristes, préc., p. 23.

son territoire. La décision étant nationale, elle sera contestée devant le juge national. De même si une enquête débute et conduit à l'ouverture d'une procédure judiciaire, ce sera une nouvelle fois une contestation des éléments du dossier devant le juge national.

24. En l'absence de décision faisant grief, la voie juridictionnelle apparait difficile à envisager, ne serait-ce que par la méconnaissance de l'utilisation des données à caractère personnel. Le seul contrôle juridictionnel efficace est, en réalité, celui de la contestation des actes de portée générale devant la Cour de justice de l'Union. En effet, la Cour de justice a montré à différentes reprises sa capacité à préserver les droits fondamentaux face aux impératifs sécuritaires. La Cour a été particulièrement attentive à la protection des données à caractère personnel, à travers plusieurs arrêts, que soient concernées des dispositions uniquement internes à l'Union européenne[46] ou qu'il s'agisse de la conclusion d'un accord international[47]. La Cour de justice a ainsi invalidé la directive sur la conservation des données adoptée en 2006. Cette directive imposait la conservation de données générées ou traitées par les fournisseurs de services de communication électronique à des fins de prévention, de recherche, de détection et de poursuites d'infractions graves. La Cour a jugé que si la sécurité publique constituait un objectif légitime afin de limiter la portée du droit à la protection des données à caractère personnel, le contenu de la directive violait clairement à plusieurs reprises la condition de la proportionnalité. La Cour a ainsi jugé que « cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire»[48]. Par cet arrêt, la Cour a réaffirmé l'exigence du respect de l'Etat droit, marquant que la lutte contre le terrorisme ne pouvait tout autoriser. L'impact de cet arrêt est très concret, la Cour imposant aux institutions de mieux encadrer les conditions de collecte et de stockage, mais surtout également les conditions d'accès. Les données ne peuvent être accessibles sans contrôle. Cette exigence ne vaut pas que pour cette directive et pose directement la question de la validité d'autres textes, dont les accords internationaux traitant de la question des échanges d'informations. Il faut préciser cependant que les accords internationaux ne peuvent pas faire l'objet directement d'un contrôle de validité dans le cadre de l'ordre juridique de l'Union. Cependant, rien n'empêche l'annulation d'une mesure d'exécution prise sur le fondement de l'un de ces accords. La portée de cet arrêt a d'ailleurs été pleinement intégrée par la Commission, au regard de sa communication sur le programme européen en matière de sécurité, divulguée postérieurement à cet arrêt. La Commission s'y engage nettement en faveur des droits fondamentaux et notamment de l'application du principe de proportionnalité L'incidence de cet arrêt est également, pour les Etats membres, non seulement pour les actes de transposition de la directive en cause comme ce fut le cas dans l'affaire *Digital Rights Ireland*[49], mais également pour toutes les autres dispositions entrant dans le champ du droit de l'Union. En effet, conformément à l'arrêt *Fransson*[50], la Cour de justice a étendu les hypothèses dans lesquelles les Etats membres sont tenus de respecter pleinement la Charte des droits fondamentaux.

25. L'effectivité de la protection des données à caractère personnel est en constante évolution sous l'impulsion, ces dernières années, du Parlement européen. Son intervention renforce le contenu des textes et joue un rôle dissuasif, aidé par la jurisprudence de la Cour de

[46] CJUE, 8 avr. 2014, *Digital Rights Ireland Ltd*, préc.
[47] CJCE, 30 mai 2006, *Parlement européen contre Conseil*, préc.
[48] CJUE, 8 avr. 2014, *Digital Rights Ireland Ltd*, *op.cit.*, § 65
[49] *Ibid.*
[50] CJUE, 26 févr. 2013, *ÅkerbergFransson c.Aklagaren*, C-617/10,ECLI:EU:C:2013:105.

justice. Toutefois, la transparence fait encore largement défaut, les individus n'étant pas en mesure de s'opposer directement aux transferts de données les concernant ou encore d'en demander la rectification, les procédures prévues étant trop succinctes ou inexistantes. L'effort devra porter sur cet aspect, tout en préservant l'exigence de sécurité.