Objectif de sécurité et protection des données personnelles: projection dans l'ordre international d'un système constitutionnel propre à l'Union européenne / Security Objective and Personal Data Protection: Constitutional Advances of a European Union-Specific System in the International Order

Laurence Potvin-Solis

Abstract

Personal data protection continuously presents key topical issues for the Union's legal order in terms of its external action and which stand out as a constitutional matter for its internal order. These issues show the extent to which the Union's external objectives must be related to its internal objectives and to the twofold dimension of the Union's external action, which develops itself both in the context of its sectorial policies and as a means for the Union to assert itself as a global and credible player on the international stage. Thus, the European Union's compliance with personal data protection is characterised by close links between the internal and external dimensions of this protection. The European Union is progressively defining its own independent approach to personal data protection, which has become progressively extended and refined within EU law. This protection is defined in Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the EU Charter of Fundamental Rights (EUCFR). In this regard, personal data protection, as well as the normative developments surrounding it, should be considered as a component of the Union's "constitutional framework", as pointed out by the Court of Justice Opinion 2/13 of 18 December 2014, which pertains to the draft agreement providing for the accession of the European Union to the Convention for the Protection of Human Rights (ECHR) and which is essential both to the Union's secondary legislation but also for negotiations aimed at concluding agreements with third countries. Recently, the Court of Justice has firmly stressed this point in Opinion 1/15 of the Grand Chamber of 26 July 2017, declaring the Canada-EU draft agreement on the transfer of Passenger Name Record (PNR) incompatible with the EUCFR.

The close link between the internal and external dimensions of personal data protection, both inside and by the European Union, is another characteristic feature of pursuing the goal of security, which must be reconciled with personal data protection requirements and can give rise to great tensions between the legal systems, as demonstrated by Opinion 1/15 of 26 July 2017. The development of tools and agreements to ensure security, particularly in the context of the fight against terrorism and serious transnational crime, calls upon the EU to define a concept of personal data protection which can be clearly identifiable in both its domestic law and its external relations. In parallel, reconciling the objective of security and the protection of personal data takes on a strong constitutional dimension in the Union's legal order, once this objective is treated, like the Union's policies and actions as a whole, in accordance with the European Union's values and fundamental rights of its respective field. Personal data protection was confirmed as a constitutional requirement by the Lisbon Treaty. Indeed, this issue is expressly governed by Article 39 TEU and Article 16 TFEU. The latter states in its first paragraph that "everyone has the right to the protection of personal data concerning them", and its second paragraph provides for the European Council and Parliament's competence to lay down, in accordance with the ordinary legislative procedure "rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data". This paragraph specifies that "the rules adopted on the basis of this article shall be without prejudice to the specific rules laid down in Article 39 of the TEU". According to the latter, "in accordance with Article 16 of the TFEU and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data". Both Article 16 TFEU and Article 39 TEU state that the "compliance with these rules shall be subject to the control of independent authorities".

Personal data protection falls within the scope of European Union law and is also associated with the scope of the EUCFR. It must be related not only to the free movement of data within the internal market of the area of freedom, security and justice (AFSJ), but also to the objectives of security and the fight against crime which, just like personal data protection, can

impact this freedom of movement and establish themselves both internally and in terms of the Union's external action. It benefits from the Lisbon Treaty's recognition of the EUCFR's legal status. Unlike the European Convention on Human Rights, in which personal data protection is covered as a fundamental right falling within the scope of Article 8 (related to the right to respect for private and family life), the Charter includes an Article that expressly applies to this type of protection. Indeed, after setting out the right to liberty and security in Article 6, and the respect for private and family life in Article 7, Article 8 of the Charter makes a provision for the protection of personal data, by stating: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Like Article 16 TFEU and Article 39 TEU, this Article sets out in its third paragraph that "compliance with these rules shall be subject to control by an independent authority".

The progress achieved in terms of a legal framework of personal data protection peculiar to the European Union and to its sectoral development goes hand in hand with the increase in personal data control, collection, conservation, and transfer instruments that aim to meet the objective of security for both the domestic order and the foreign relations of the European Union. This progress is driven by the closer ties and tensions between the European Union, its Member States, and third countries. It must meet the increasing requirements of the case law of the Court of Justice of the European Union. It presents a challenge of coherence for the Union's legal system (as laid out by Article 13 TEU), since it affects not only the values on which it is founded (in particular as stated in Article 2 TEU), such as the respect for freedom, democracy, the rule of law, and human rights, but also applies to all of the Union's actions, internal or external. Promoting these values is the first of the objectives set out in Article 3 TEU. To handle the divergent views between Member States and the international arena, the autonomy of the European Union, its law and its Court of Justice are put forward, especially when it comes to reconciling personal data protection and the objectives of security with the scope of international order, so as to be consistent with its constitutional internal framework. The international terms under which the promotion of these values is laid out cannot be disassociated from the necessary assertion of a sys-

tem of protection peculiar to the European Union to ensure the respect for fundamental rights related to personal data processing, access, retention, alteration, and transfer, as well as the right to be forgotten.

This contribution brings to light the identification details and constitutional nature of such a system of protection peculiar to the European Union, with regard to requirements of the Court of Justice's jurisprudence and to developments of the Union's regulatory framework and of their external repercussions. It includes the challenges of negotiating the international agreements and ongoing reforms as well as the input of Opinion 1/15 of the Grand Chamber of 26 July 2017 regarding the agreement envisaged between Canada and the European Union on the transfer and processing of Passenger Name Record data. It highlights the imperative of a global approach to the relationship between personal data protection and the pursuit of the objective of security, an approach that can be defined and carried out by the European Union in its foreign relations and as an expression of its identity in the international arena.

The paper firstly analyses the European Union's appropriation of the constitutional terms for reconciling data protection with the pursuit of these objectives. In this context, it considers the necessity for the European Union to provide consistency: (*a*) In its pursuit of a high level of personal data protection in its general and sectoral regulations and their external aspects; (*b*) In its control of the interdependence of internal and external challenges of reconciling the European Union's general and sectoral objectives; and (*c*) In the autonomy of assessment set in the European Union's constitutional framework relating to the interpretation of the fundamental rights and concepts governing personal data protection and the increasing control of the objectives which justifies interferences.

Secondly, the contribution analyses the advances of a European constitutional identity as a consequence of the assertion of a system of protection peculiar to the European Union. To this effect, it considers: (*a*) The internal and external scope of constitutional advances achieved by the Court of Justice's jurisprudence that act in favour of personal data protection; (*b*) The broad implications of constitutional requirements regarding the independence of supervisory authorities within the European Union, its Member States and towards third-countries; And (*c*) The increasingly unique characteristics of the European Union's system of protection as a result of the relationship between the objectives and the legal bases and the necessity to ensure a continuity in personal data protection that is

equivalent and suited to the high level of protection within the European Union.

***

La protection des données personnelles présente des enjeux de constante actualité pour l'ordre juridique de l'Union européenne sous l'angle de son action extérieure et qui s'imposent comme une question constitutionnelle pour son ordre interne. Ces enjeux montrent combien les objectifs externes de l'Union doivent être rapportés à ses objectifs internes et à la double dimension de l'action extérieure de l'Union qui se développe tant dans le cadre de ses politiques sectorielles que comme moyen d'affirmation de l'Union en tant qu'acteur global identifiable et crédible sur la scène internationale. Ainsi, le respect par l'Union européenne de la protection des données personnelles est caractérisé par une très forte imbrication entre les dimensions interne et externe de cette protection. L'Union européenne définit progressivement une conception autonome de la protection des données personnelles qui lui est propre et qui s'est trouvée progressivement élargie et affinée en droit de l'Union. Cette protection fait aujourd'hui l'objet de l'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE) et de l'article 8 de la Charte des droits fondamentaux de l'Union européenne (CDFUE). Elle doit en cela et dans les développements normatifs dont elle fait l'objet, être perçue comme une composante du « cadre constitutionnel » de l'Union mis en avant par la Cour dans l'avis 2/13[1], qui s'impose tant au droit dérivé de l'Union que dans le cadre des négociations en vue de la conclusion d'accords avec les États tiers, comme l'a rappelé fermement la Cour de justice dans son avis 1/15, constatant l'incompatibilité avec la CDFUE du projet d'accord entre le Canada et l'Union européenne sur le transfert des données des dossiers passagers aériens depuis l'Union vers le Canada[2].

La forte imbrication entre les dimensions interne et externe de la protection des données personnelles dans et par l'Union caractérise également

1 Avis de la Cour du 18 décembre 2014, 2/13, *Projet d'accord d'adhésion de l'Union européenne à la Convention européenne des droits de l'homme*, EU:C:2014:2454, points 155 à 177.

2 Avis de la Cour du 26 juillet 2017, 1/15, *Transfert des données des dossiers passagers aériens depuis l'Union vers le Canada*, EU:C:2017:592. V. nos développements *infra*.

la poursuite de l'objectif de sécurité qui doit être concilié avec les exigences de cette protection et qui est source de vives tensions entre les ordres juridiques, comme le montre l'avis 1/15. Le développement des instruments et des accords au service de la sécurité, tout particulièrement dans le cadre de la lutte contre le terrorisme et contre la criminalité transnationale grave, invite l'Union à définir une conception de la protection des données à caractère personnel qui puisse être clairement identifiable dans son ordre interne comme dans ses relations extérieures. La conciliation entre l'objectif de sécurité et la protection des données personnelles revêt en même temps une forte dimension constitutionnelle dans l'ordre juridique de l'Union dès lors que cet objectif est rapporté, comme l'ensemble des politiques et actions de l'Union, au respect des valeurs de l'Union et des droits fondamentaux dans son champ[3]. La protection des données personnelles a été confortée comme exigence constitutionnelle par le traité de Lisbonne. Elle est en effet expressément régie par l'article 39 du Traité sur l'Union européenne (TUE) et par l'article 16 TFUE. Ce dernier énonce, dans son premier paragraphe, que « toute personne a droit à la protection des données à caractère personnel la concernant » et son deuxième paragraphe prévoit la compétence pour adopter, sur la base de la procédure législative ordinaire, « les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données ». Ce paragraphe précise que « les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 TUE ». Selon ce dernier, « conformément à l'article 16 TFUE et par dérogation à son paragraphe 2, le Conseil adopte une décision fixant les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du présent chapitre, et à la libre

3 R. Tinière, C. Vial (dir.), *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Bruylant, Bruxelles, Coll. Droit de l'Union européenne, 2015; L. Potvin-Solis (dir.), *Les valeurs communes dans l'Union européenne, Onzièmes Journées Jean Monnet,* Bruylant, Bruxelles, Colloques Jean Monnet, 2014; L. Potvin-Solis (dir.), *Politiques de l'Union européenne et droits fondamentaux, Treizièmes Journées Jean Monnet,* Bruylant, Bruxelles, Colloques Jean Monnet, 2016.

circulation de ces données ». Les articles 16 TFUE et 39 TUE précisent tous deux que « le respect de ces règles est soumis au contrôle d'autorités indépendantes ».

La protection des données personnelles est donc source d'obligations pour l'Union et pour ses États membres et donne lieu à un titre de compétence expressément affirmé au bénéfice de l'Union et à l'égard des États membres. Son champ se conjugue au champ d'application du droit de l'Union et implique celui de la Charte des droits fondamentaux de l'Union. Elle doit être rapportée tant à la libre circulation des données au sein du marché intérieur et de l'espace de liberté, de sécurité et de justice qu'aux objectifs de sécurité et de lutte contre la criminalité qui peuvent, comme elle, agir sur cette liberté de circulation. Qui plus est, elle bénéficie de la reconnaissance par le traité de Lisbonne de la valeur juridique de la Charte qui, à la différence de la Convention européenne des droits de l'homme[4] comporte un article qui lui est expressément consacré. La Charte prévoit en effet, après le droit à la liberté et à la sûreté énoncés dans son article 6, et le respect de la vie privée et familiale garanti par son article 7, la protection des données à caractère personnel, dans son article 8, selon lequel :

«1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces 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. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification [...]».

Comme les articles 16 TFUE et 39 TUE, cet article pose dans son troisième paragraphe que « le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Les progrès d'un cadre légal de protection des données personnelles propre à l'Union s'imposent de façon corrélative à l'accroissement des instruments de contrôle, de collecte, de conservation et de transfert des données personnelles visant à répondre à l'objectif de sécurité dans l'ordre interne et dans l'action extérieure de l'Union. Ils se nourrissent des rapprochements et des tensions entre l'Union, ses États membres et les États

4 La Convention couvre la protection des données personnelles comme droit fondamental compris dans le champ d'application de son article 8 sur le droit au respect de la vie privée et familiale.

tiers et doivent répondre aux exigences grandissantes de la jurisprudence de la Cour de justice. Ils représentent un enjeu de cohérence pour l'ordre juridique de l'Union d'autant plus qu'ils touchent aux valeurs qui sont placées à ses fondements, telles que le respect de l'État de droit et des droits de l'homme, et qui s'imposent à toutes ses actions, internes et externes. Ils conduisent l'Union à définir une protection autonome et « son » identité par les développements progressifs d'une harmonisation des législations nationales au sein du marché intérieur, de ses politiques et de l'espace de liberté, de sécurité et de justice et d'exigences qui lui sont propres dans le cadre de son action extérieure et de ses négociations pour la conclusion d'accords internationaux avec les États tiers. La protection des données personnelles suscite un intérêt croissant et de vifs débats dans un contexte international marqué par les contestations qui se sont élevées face à des pratiques de surveillance et de collecte de données de masse, telles que les écoutes de la *National Security Agency (NSA)*. Face aux divergences de conception en présence, l'autonomie de l'Union, de son droit et de son juge est mise en avant, tout particulièrement lorsqu'il s'agit de concilier la protection des données personnelles aux objectifs de sécurité dans l'ordre international en cohérence avec son ordre interne. La protection des données personnelles obéit alors à un raisonnement similaire à celui mené dans l'arrêt *Kadi* marquant l'autonomie du contrôle juridictionnel de la garantie des droits fondamentaux dans l'Union européenne[5]. Les termes internationaux dans lesquels elle se pose à l'Union ne peuvent être dissociés de l'affirmation nécessaire d'un système de protection propre à l'Union pour le respect des droits fondamentaux en matière d'accès, de conservation (et d'oubli) et de transfert.

C'est donc à partir d'une mise en relief des éléments d'identification de ce système et de la mise en exergue de sa nature « constitutionnelle » pour l'Union que sera ici analysée la protection des données personnelles rapportée aux objectifs de sécurité de l'Union. Les enjeux constitutionnels des termes de la conciliation des intérêts s'imposent à chaque étape des progrès du droit dérivé et sont mis en relief devant la Cour de justice. Par sa jurisprudence, au sein de laquelle tous les intérêts convergent, la Cour encadre la marge d'appréciation des autorités publiques des États membres et de l'Union en prenant en considération les aspects généraux et sec-

5 Arrêt de la Cour du 3 septembre 2008, *Kadi et Al Barakaat International Foundation/Conseil et Commission,* C-402/05 P, EU:C:2008:461.

toriels ainsi que les dimensions internes et externes. C'est sous l'impulsion du développement d'un cadre juridique spécifique à l'Union qu'ont été progressivement révélés les traits d'un système constitutionnel propre à l'Union et identifiable comme tel dans l'ordre international. Les apports de la jurisprudence toujours plus étoffée de la Cour de justice occupent une place centrale dans cette évolution qui traduit les prolongements externes des finalités internes de l'Union. Les enjeux généraux et transversaux des réformes en cours dans l'Union et des négociations par l'Union d'accords internationaux portant sur les données personnelles montrent la nécessité d'une appropriation par l'Union des termes constitutionnels de la conciliation des objectifs (I) qui puisse trouver un fondement solide par l'affirmation d'un système constitutionnel propre à l'Union et à même d'exprimer son identité sur la scène internationale (II).

I. L'appropriation par l'Union des termes constitutionnels de la conciliation des objectifs

La jurisprudence de la Cour de justice permet d'affiner les termes de cette conciliation. Les progrès d'un cadre général de protection des données personnelles dans l'Union se combinent avec les développements sectoriels de cette protection. Ils sont par ailleurs marqués, d'un point de vue général comme sur le plan sectoriel, par la forte imbrication entre les dimensions internes et externes de la conciliation entre les objectifs et entre les intérêts en présence. Ils forment donc un enjeu de taille pour la cohérence du cadre normatif de l'Union et pour l'autonomie de la garantie et de l'interprétation des droits fondamentaux par l'Union. Cette interprétation doit être menée par référence au cadre constitutionnel de l'Union au sens de l'avis 2/13 sur le projet d'accord d'adhésion de l'Union à la Convention européenne des droits de l'homme[6]. Elle doit permettre d'assurer la cohérence dans la poursuite d'un niveau élevé de protection des données personnelles (A) et la maîtrise par l'Union de l'interdépendance des enjeux internes et externes de la conciliation entre la protection des données personnelles et les objectifs de sécurité (B). Elle exprime toujours davantage une autonomie d'appréciation ancrée dans le cadre constitutionnel de l'Union (C).

6 Avis de la Cour du 18 décembre 2014, 2/13, *supra* note 1.

A. La cohérence dans la poursuite d'un niveau élevé de protection des données personnelles

Les exigences de cohérence sont multiples et invitent l'Union à mener une approche globale de la protection des données personnelles et à en développer une conception autonome y compris lorsqu'elle est rapportée aux objectifs de sécurité. Telle qu'elle est posée dans l'article 13 TUE, cette cohérence doit être rapprochée de la promotion par l'Union de ses valeurs, de la poursuite de ses objectifs et de la réalisation de « ses intérêts, ceux de ses citoyens, et ceux des États membres ». Elle est affirmée en lien avec la nécessité pour l'Union d'assurer « l'efficacité et la continuité de ses politiques et de ses actions ». Elle s'impose à l'action extérieure de l'Union mais ne peut être conçue qu'en partant de son ordre interne. Elle s'est trouvée progressivement affirmée, tant dans les rapports entre la règlementation applicable aux États membres et celle applicable à l'Union (1) que dans l'articulation entre la règlementation générale et les règlementations sectorielles de l'Union (2).

1. La cohérence entre la règlementation applicable aux États membres et celle applicable à l'Union

Concernant les États, la directive 95/46/CE 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 a constitué le texte de base[7]. Selon la Cour de justice, cette directive a abouti « à une harmonisation qui est, en principe, complète » et ne se limite pas à une harmonisation minimale même si elle comporte « des règles caractérisées par une certaine souplesse laissant dans de nombreux cas aux États membres le soin d'arrêter les détails ou de choisir parmi des options » et préserve donc une certaine marge d'appréciation nationale[8]. Elle a imposé cette protection au sein des échanges entre les États membres, face aux progrès des technolo-

7 Directive 95/46/CE du Parlement européen et du Conseil, *JO* L 281, du 23 novembre 1995, p. 31.

8 V. not. : Arrêt de la Cour du 6 novembre 2003, *Lindqvist,* C-101/01, EU:C:2003:596, points 95 et 96; Arrêt de la Cour du 16 décembre 2008, *Huber,* C-524/06, EU:C:2008:724, points 50 et 51; Arrêt de la Cour du 7 mai 2009, *Rijkeboer,* C-553/07, EU:C:2009:293, point 56.

gies de la communication et comme corollaire de la garantie des droits fondamentaux dans les États. Elle a contribué à l'objectif de cohérence dès lors qu'elle a cherché à assurer « un niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données » qui soit « équivalent dans tous les États membres »[9] en visant l'objectif d'un niveau de protection élevé à partir duquel la Cour de justice exerce son contrôle[10]. La directive 95/46/CE a été abrogée et remplacée par le règlement général sur la protection des données personnelles n° 2016/679/UE (RGPD),[11] entré en application le 25 mai 2018. Ce règlement poursuit le mouvement d'unification du cadre juridique de l'Union et contribue à renforcer les droits des personnes[12] et les obligations qui pèsent sur les responsables du traitement des données et sur les sous-traitants ainsi que les conditions tenant à l'indépendance des autorités de contrôles[13], la coopération et la cohérence[14]. Il procède à une modernisation de la directive qui a donné lieu à une importante jurisprudence dont il reprend certaines avancées et s'inscrit dans un mouvement de réforme plus large[15].

Vis-à-vis de l'Union, le règlement n° 45/2001/CE relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données a également posé l'objectif d'un niveau de protection élevé des données à caractère personnel[16]. Il vise à « assurer dans l'ensemble de la Communauté une application cohérente et homogène des

9 Cons. 8 de la directive.

10 Arrêt de la Cour du 13 mai 2014, *Google Spain et Google,* C-131/12, EU:C:2014:317, point 66.

11 Règlement n° 2016/679/UE 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 (règlement général sur la protection des données), *JO* L 119, du 4 mai 2016, p. 1.

12 En matière de droit d'accès, de rectification, de suppression (avec le droit à l'oubli ou le droit à l'effacement), d'opposition, de droit de limitation du traitement des données, de droit à la portabilité des données personnelles ou encore les droits en matière de profilage.

13 V. le chap. VI du règlement.

14 V. le chap. VII du règlement.

15 V. not. la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016, *JO* L 119, du 4 mai 2016, p. 89 et la directive 2016/681/UE du Parlement européen et du Conseil du 27 avril 2016, *JO* L 119, du 4 mai 2016, p. 132.

16 Règlement n° 45/2001/UE du Parlement européen et du Conseil du 18 décembre 2000, *JO* L 8, du 12 janvier 2001, p. 1.

règles de protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel »[17]. Il reste applicable au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union après l'intervention du règlement n° 2016/679/UE. Mais ce dernier prévoit que, comme les autres actes juridiques de l'Union régissant le traitement des données à caractère personnel, il doit être adapté « aux principes et aux règles »[18] qu'il fixe et il exige leur réexamen « afin d'assurer une protection uniforme et cohérente des personnes physiques à l'égard du traitement » en précisant que « cela concerne en particulier les règles relatives à la protection des personnes physiques à l'égard du traitement par des institutions, organes et organismes de l'Union et à la libre circulation de ces données »[19].

2. *La cohérence entre la réglementation générale et les règlementations sectorielles de l'Union*

Certaines règlementations sectorielles ont pour objet même la protection des données personnelles dans un champ spécifique tandis que d'autres poursuivent des objectifs d'ordre sécuritaire mais intègrent la protection des données personnelles dans les dispositifs de contrôle qu'elles mettent en place. Dans le domaine des communications électroniques, la protection des données personnelles a été prévue par la directive 97/66/CE[20] à laquelle renvoie la directive sur le commerce électronique 2000/31/CE[21], puis par la directive 2002/58/CE[22], qui comporte notamment des dispositions relatives à la conservation des données de connexion par les États membres à des fins de surveillance policière**.** Ces directives peuvent susciter des questions d'interprétation liées à celle de la règlementation

17 *Id.*, considérant 12.
18 Article 2, paragraphe 3 du règlement n° 2016/679*, supra* note 11.
19 *Id.*, article 98.
20 Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *JO* L 24, du 30 janvier 1998, p. 1.
21 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000, *JO* L 178, du 17 juillet 2001, p. 1, cons. 14 et s.
22 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, *JO* L 201, du 31 juillet 2002, p. 37.

générale des données personnelles dans l'Union[23] et au respect de la Charte des droits fondamentaux de l'Union. La Cour de justice a notamment jugé dans l'arrêt *Tele2 Sverige* que l'article 15 paragraphe 1 de la directive 2002/58/CE s'oppose à « une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique »[24]. Cette directive fait l'objet d'une réforme en cours qui marque les imbrications entre les objectifs généraux et les objectifs sectoriels. Elle doit en effet être abrogée par un réglement *ePrivacy* qui vise à développer l'harmonisation des législations nationales en matière de confidentialité des communications électroniques et à garantir un niveau élevé de protection des données issues de ces communications afin de ne pas réduire celui garanti par le RGPD. Cette proposition de règlement « vie privée et communications électroniques » constitue donc un pas supplémentaire dans le processus d'harmonisation dans ce secteur et est orientée vers les objectifs de la stratégie pour le marché unique numérique. Le retard pris dans son adoption témoigne de la force des résistances qu'elle suscite de la part des milieux professionnels concernés. Elle vise à actualiser les dispositions de la directive 2002/58/CE et à en étendre le champ à l'ensemble des fournisseurs de services de communications électroniques. Les questions de cohérence ont notamment été soulevées par le contrôleur européen de la protection des données (CEPD) dans son avis rendu sur la proposition de règlement *ePrivacy*. Il les a notamment relevées en ce qui concerne la détermination du sens même des notions sur lesquelles cette proposition repose dans la mesure où leurs définitions devront être posées dans « le code des communications électroniques européen » et seront donc « centrées sur la concurrence et le marché », et, dès lors, selon le CEPD, mal « adaptées au contexte des

23 V. not. le renvoi préjudiciel introduit par le Bundesgerichtshof le 30 novembre 2017, *Planet49 GmbH.,* C-673/17.

24 Arrêt de la Cour du 21 décembre 2016, C-203/15 et C-698/15, EU:C:2016:970. Sur cette jurisprudence et les questions d'interprétation de la directive 2002/58/CE au regard des droits fondamentaux et de la CEDH, v. not. le renvoi préjudiciel introduit par le Investigatory Powers Tribunal-London le 31 octobre 2017, *Privacy International,* C-623/17.

droits fondamentaux »[25]. Les questions de cohérence entre la réglementation générale et les règlementations sectorielles de l'Union se mesurent à l'aune du nombre d'avis rendus par le CEPD des données, comme en témoignent par exemple, l'avis sur la proposition d'un cadre commun pour des statistiques européennes relatives aux personnes et aux ménages[26] ou, de façon toute particulière, l'avis sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*) qui en souligne les enjeux en termes de légalité, de responsabilité et de valeurs[27].

Les règlementations sectorielles de l'Union qui visent des objectifs de sécurité peuvent concerner des secteurs aussi variés que le secteur bancaire, le secteur financier et fiscal (et pour la protection des données fiscales, l'assistance administrative internationale), le secteur du E-commerce, celui de la santé et de la E-santé, le cyberespace et internet, la lutte contre la fraude, ou encore la propriété intellectuelle[28]. La question de la protection des données personnelles fait aussi l'objet de dispositions particulières en matière pénale, dans des textes généraux[29] et dans des actes spécifiques comme la décision cadre 2008/977/JAI relative à la protection des données traitées dans le cadre de la coopération judiciaire et policière en matière pénale[30]. Cette décision-cadre a été abrogée et remplacée par la directive 2016/680/UE 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 sanc-

25 Avis du Contrôleur européen de la protection des données du 24 avril 2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (2017/C 234/03), *JO* C 234, du 20 juillet 2017, p. 3.

26 Avis du Contrôleur européen de la protection des données du 1er mars 2017 (2017/C87/01), *JO* C 87, du 21 mars 2017, p. 1.

27 Avis 8/2016 du 23 septembre 2016. V. aussi le *Rapport annuel du contrôleur européen de la protection des données*, Luxembourg, Office des publications de l'Union européenne, 2017.

28 V. le séminaire qui s'est tenu à la Cour de justice de l'Union, les 18-20 septembre 2014 sur « les enjeux européens et mondiaux de la protection des données personnelles ».

29 V. not. l'article 10 du règlement général sur la protection des données personnelles 2016/679, *supra* note 11.

30 Décision cadre 2008/977/JAI du Conseil du 27 novembre 2008, *JO* L 350, du 30 décembre 2008, p. 60.

tions pénales[31]. La protection des données personnelles est également directement concernée par les instruments normatifs qui se sont développés dans le domaine de la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme[32]. Par exemple, la quatrième directive intervenue dans ce domaine, la directive 2015/849/UE, prévoit une évaluation des risques qui repose sur une coopération et des échanges de données avec les États membres qui doivent être respectueux des droits fondamentaux et de la protection des données personnelles[33]. Cette directive pose des exceptions et restrictions au droit d'accès justifiées par l'objectif d'efficacité dans la poursuite de ses objectifs. Elle a fait l'objet d'une proposition de directive modificative[34] qui étend la prise en compte des risques à ceux provenant de l'utilisation de nouvelles technologies dans les transactions financières, qui permet un renforcement et une harmonisation des contrôles exercés sur les flux financiers provenant de pays tiers à haut risque, et qui accroît les exigences de transparence et les compétences des cellules de renseignement financier des États membres. Dans son avis du 2 février 2017 sur cette proposition de directive, le CEPD a rappelé les exigences du principe de proportionnalité et du « principe de limitation de la finalité ». Il a souligné notamment que « le traitement de données à caractère personnel recueillies à certaines fins pour d'autres fins, sans aucun lien avec les premières, constitue une infraction au principe de protection des données de limitation de la finalité et menace l'application du principe de proportionnalité ». Selon cet avis, les modifications prévues « soulèvent en particulier la question de savoir pourquoi certaines formes de traitement invasif des données à caractère personnel, acceptables quand il est question de lutte contre le blanchiment de capitaux et contre le terrorisme, sont néces-

31 Cette directive (*supra* note 15) est entrée en vigueur le 5 mai 2016 et doit être transposée au plus tard le 6 mai 2018.

32 V. not. L. Potvin-Solis, « La lutte contre le terrorisme et son financement : la nécessité d'un cadre constitutionnel renforcé », *Revue du droit de l'Union européenne,* n°3/2017, p. 11.

33 Cons. 65 et 66 de la directive.

34 Proposition de directive du Parlement européen et du Conseil modifiant la directive 2015/849 et la directive 2009/101/ CE, COM(2016) 450 final du 5 juillet 2016. V. not. Avis du Parlement européen du 30 janvier 2018 sur la base juridique de cette proposition de directive, PE 616.787 v 01-00-C8-0265/2016.

saires en-dehors de ces contextes et si elles sont proportionnées »[35]. La protection des données personnelles se pose dans les mêmes termes au sein du dispositif de l'Union visant à assurer la traçabilité des virements de fonds et des mouvements de liquidités. Le règlement n° 1889/2005/CE vise à renforcer les contrôles de l'argent liquide entrant ou sortant de l'Union.[36] Le règlement n° 2015/847/UE détermine les conditions relatives à l'obtention et à la conservation des données et leur protection en ce qui concerne les informations accompagnant les transferts de fonds. Il prévoit que ces conditions doivent respecter la directive 95/46/CE et le règlement n° 45/2001/CE. Une proposition a été adoptée par la Commission en décembre 2016 pour un nouveau règlement relatif aux contrôles d'argent liquide entrant dans l'Union ou sortant de l'Union[37]. Les exigences de cohérence sont d'autant plus prégnantes que la matière est mouvante et en cours de réforme d'ensemble.

La jurisprudence de la Cour de justice peut préciser l'articulation entre la protection générale des données personnelles et les instruments juridiques catégoriels ou sectoriels. Elle contribue à la cohérence d'ensemble notamment quand elle procède par des rapprochements entre les interprétations jurisprudentielles entre elles. Par exemple, dans l'arrêt *Institut professionnel des agents immobiliers*[38], la Cour de justice interprète l'article 13, paragraphe 1, de la directive 95/46/CE qui prévoit des exceptions à l'obligation d'informer les personnes concernées du traitement de leurs données à caractère personnel, par référence à l'interprétation donnée dans son arrêt *Promusicae* de l'article 15, paragraphe 1, de la directive « vie privée et communications électroniques »[39]. Elle juge que cette disposition ne contient pas une obligation mais une faculté pour les États de transposer dans leur droit national une ou plusieurs des exceptions qu'elle

35 Avis 1/2017 du Contrôleur européen de la protection des données du 2 février 2017, *JO* C 162, du 23 mai 2017, p. 9.

36 Règlement n° 1889/2005/CE du Parlement européen et du Conseil du 26 octobre 2005, *JO* L 309, du 25 novembre 2005, p. 9. V. not. Potvin-Solis, « La lutte contre le terrorisme et son financement », *supra* note 30, p. 41 et s.

37 Proposition de règlement abrogeant le règlement n° 1889/2005/CE, COM (2016) 825 final; v. les commentaires du Contrôleur européen de la protection des données du 21 février 2017.

38 Arrêt de la Cour du 7 novembre 2013, *Institut professionnel des agents immobiliers* (*IPI*), C-473/12, EU:C:2013:715.

39 Arrêt de la Cour du 29 janvier 2008, *Promusicae*, C-275/06, EU:C:2008:54.

mentionne[40] et que l'activité de détective privé dont il était question entre dans son champ[41].

B. La maîtrise de l'interdépendance des enjeux internes et externes de la conciliation

Nombreux sont les secteurs impliqués dans leurs dimensions interne et externe par la protection des données personnelles et les avancées de la règlementation de l'Union. Les développements du droit dérivé et de la jurisprudence fixent l'étendue des obligations qui pèsent sur les États et sur l'Union et permettent d'affiner toujours davantage les modalités de la protection des données personnelles et le cadre légal des ingérences dans les droits fondamentaux justifiées par des objectifs de sécurité. Les progrès du cadre normatif de l'Union en matière de transfert des données personnelles illustrent parfaitement cette évolution vers une appropriation par l'Union des termes constitutionnels de la conciliation des intérêts et des droits en présence et des conditions de la rencontre entre les enjeux internes et externes de cette conciliation. Les avancées de la règlementation générale à l'égard des États membres et de l'Union (1) présentent en effet des enjeux similaires à ceux qui dominent la poursuite par l'Union de ces objectifs dans ses relations extérieures et dans la négociation et la conclusion d'accords internationaux, comme en témoigne l'avis 1/15 rendu par la Cour de justice sur le projet d'accord entre le Canada et l'Union européenne sur le transfert des données des dossiers passagers aériens depuis l'Union vers le Canada (2).

1. L'interdépendance dans la règlementation générale à l'égard des États membres et de l'Union

La directive 95/46/CE marquait déjà l'imbrication entre les dimensions internes/externes de la protection des données personnelles par la notion même d'établissement permettant de couvrir l'établissement dans un pays tiers du responsable du traitement de données. Selon son considérant 20,

---

40 Arrêt de la Cour du 7 novembre 2013, *Institut professionnel des agents immobiliers* (*IPI*), *supra* note 38, point 37.

41 *Id.,* point 34.

cet établissement ne doit pas contrarier la protection qu'elle met en place, et que les traitements de données personnelles doivent alors être soumis à la loi de l'État membre où sont localisés les moyens utilisés pour ces traitements et respecter « des garanties » pour que les droits et obligations posés par cette directive « soient effectivement respectés ». Cette même imbrication apparaît aussi dans les dispositions de la directive relatives aux transferts de données à caractère personnel d'un État membre de l'Union vers un État tiers qui imposent que les transferts ne soient autorisés que si « ce dernier assure un niveau de protection adéquate ». Si tel n'est pas le cas, de tels transferts ne peuvent en principe être opérés sauf dérogations limitativement énumérées. Cette condition se retrouve dans les décisions relatives aux clauses contractuelles types pour le transfert des données vers des pays tiers en vertu de la directive 95/46/CE[42], dès lors que ces clauses visent à assurer des garanties adéquates lors du transfert des données à caractère personnel de l'Union européenne vers des États tiers.

La directive PNR 2016/681/UE complète la directive 2004/82/CE relative à l'obligation pour les transporteurs de communiquer les données relatives aux passagers dans le cadre de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration illégale. Elle vise à « créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes ». Elle rappelle le respect du principe de proportionnalité entre la protection des données personnelles et les objectifs spécifiques de sécurité qu'elle vise ainsi que le respect des droits fondamentaux, par référence à la Charte, en particulier ses articles 8, 7 et 21, du droit à la protection des données à caractère personnel, du droit au respect de la vie privée et du droit à la non-discrimination. Elle précise son articulation avec la directive 2004/82/CE, avec le droit de l'Union et le droit national concernant le principe de l'accès du public aux documents officiels ou encore avec la décision-cadre 2008/977/JAI. Elle précise qu'elle peut exiger, pour le respect du principe de proportionnalité et « pour des points spécifiques, des règles de protection des données plus strictes ». Lorsqu'il s'est prononcé sur la proposition de directive adoptée

42 Décision 2001/497/CE de la Commission du 15 juin 2001, *JO* L 181, du 4 juillet 2001, p. 19, et décision 2004/915/CE du 27 décembre 2004 la modifiant, *JO* L 385, du 29 décembre 2004, p. 74.

par la Commission[43], le contrôleur européen de la protection des données personnelles a souligné les risques présentés par une utilisation qui serait « systématique et sans discernement pour tous les passagers », et a mis en évidence la nécessité d'en limiter le champ d'application, de définir davantage la nature des différentes menaces autorisant l'échange de données et d'introduire un niveau de protection élevé par référence à la directive 95/46/CE. Il a invité à limiter la durée de conservation des données à 30 jours « sous une forme identifiable, sauf dans les cas nécessitant une enquête plus approfondie » et à réduire la liste des données PNR à traiter. Il a également appelé à un renforcement des conditions relatives à l'évaluation de la directive. Concernant l'imbrication entre les enjeux internes et externes de la protection des données personnelles, il a recommandé que les développements relatifs à un système PNR au niveau de l'Union soient évalués « dans une perspective plus large, incluant l'évaluation générale actuelle de l'ensemble des instruments européens dans le domaine de la gestion de l'échange de l'information mise en œuvre par la Commission »[44]. Le lien entre les enjeux internes et externes s'observe dans la jurisprudence lorsque la Cour de justice exerce son contrôle, sur la base de la directive PNR 2016/681/UE, du respect par les institutions de l'Union du droit à la protection des données personnelles. Il s'observe également dans le règlement général sur la protection des données 2016/679/UE[45] et dans la directive 2016/680/UE relative à la protection des données à caractère personnel dans le cadre de la coopération en matière pénale qui consacrent tous deux dans des termes identiques leur chapitre V aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales[46].

43 Proposition de la Commission du 2 février 2011 de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers des passagers, COM(2011) 32 final.

44 Avis du Contrôleur européen de la protection des données du 25 mars 2011 (2011/C/ 181/02), *JO* C 181, du 22 juin 2011, p. 24.

45 *Supra* note 11.

46 *Supra* note 15.

2. *L'interdépendance dans le cadre des accords internationaux de l'Union européenne*

Les accords internationaux conclus par l'Union tendent à se multiplier dans le cadre d'une stratégie extérieure de l'Union reposant sur une « démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers »[47]. Cette stratégie a donné l'occasion au CEPD de mettre en avant la nécessité « d'assurer une cohérence entre les différentes initiatives directement ou indirectement liées au traitement des données PNR », de prévoir de façon plus précise les garanties minimales applicables aux accords internationaux et d'imposer que ces derniers comportent des droits directement applicables[48]. Le CEPD est amené à se prononcer sur de tels accords[49]. La Cour de justice peut être saisie pour statuer sur leur compatibilité avec le droit de l'Union et le bien-fondé de la base juridique retenue pour leur conclusion. Ainsi, l'arrêt *Parlement/Conseil*[50] a annulé la décision 2004/496/CE du Conseil, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis 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 ainsi que la décision 2004/535/CE de la Commission, qui constatait le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique.

Plus récemment, la Cour de justice a été saisie d'une demande d'avis introduite par le Parlement européen[51] sur la compatibilité avec le droit de

47 Communication de la Commission du 21 septembre 2010, COM(2010)492 final.

48 Avis du contrôleur européen de la protection des données du 19 octobre 2010, *JO* C 357, du 30 décembre 2010, p. 7.

49 V. not. les avis du Contrôleur européen de la protection des données : du 15 juillet 2011, sur la proposition de décision du Conseil relative à la conclusion de l'accord *PNR* entre l'UE et l'Australie, *JO* C 322 du 5 novembre 2011, p. 1; du 9 décembre 2011, sur la proposition de décision du Conseil relative à la conclusion de l'accord PNR entre les États Unis d'Amérique et l'UE, *JO* C 35, du 9 février 2012, p. 16; du 30 septembre 2013, sur la proposition de décision du Conseil relative à la conclusion et à la signature de l'accord entre le Canada et l'UE sur le transfert et le traitement des données des dossiers passagers, *JO* C 51, du 22 février 2014, p. 12.

50 Arrêt de la Cour du 30 mai 2006, *Parlement/Conseil et Commission,* C-317/04 et C-318/04, EU:C:2006:346, v. nos développements *infra*.

51 En vertu de l'article 218, paragraphe 11, TFUE.

l'Union de la décision relative à l'accord entre l'Union et le Canada pour le transfert et le traitement des données de dossiers passagers dans le cadre de la lutte contre le terrorisme et la criminalité transnationale grave. La Cour devait se prononcer sur la compatibilité de cet accord avec l'article 16 TFUE et les articles 7, 8 et 52 paragraphe 1, CDFUE et sur le bien-fondé de la base juridique retenue et l'articulation entre l'article 82, paragraphe 1, d) et l'article 87, paragraphe 2, a) TFUE d'une part, et l'article 16 TFUE qui porte spécifiquement sur le droit à la protection des données personnelles, d'autre part. L'Avocat général Paolo Mengozzi proposait à la Cour de poursuivre dans le sens des progrès de son contrôle juridictionnel réalisés par ses arrêts *Digital Rights Ireland et Seitlinger e.a.*[52] et *Schrems*[53] en appliquant un contrôle strict du respect des articles de la Charte invoqués et de n'admettre que des restrictions strictement nécessaires à la réalisation de l'objectif sécuritaire poursuivi par l'accord[54]. Dans son avis 1/15 la Cour constate l'incompatibilité de cet accord avec les articles 7, 8, 21 et 52, paragraphe 1, de la Charte. Cette incompatibilité tient en premier lieu à ce qu'il peut concerner des données sensibles dont le transfert est pourtant interdit par le droit de l'Union. L'exclusion de ces données sensibles du champ du transfert conditionne la compatibilité de l'accord avec le droit de l'Union qui doit par ailleurs respecter les droits fondamentaux et le principe de proportionnalité. Après avoir relevé que cet accord constitue une ingérence dans les articles 7 et 8 de la Charte, la Cour rappelle que l'article 52, paragraphe 1 de la Charte exige que toute limitation aux droits et libertés qu'elle protège soit prévue par la loi et respecte leur contenu essentiel et le principe de proportionnalité, strictement contrôlé. La Cour précise alors de façon détaillée les conditions de compatibilité de cet accord avec les articles 7, 8 et 52 paragraphe 1 de la Charte. Le même type de problématique soulevant des questions de cohérence dans la garantie des droits fondamentaux et de la protection des données personnelles se pose au regard des progrès déjà envisagés des instruments normatifs de l'Union pour lutter contre le blanchiment et le financement du terrorisme et pour assurer la traçabilité des virements de fonds et des mouvements de liquidités. Ces objectifs peuvent donner lieu à

52 Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.,* C-293/12 et C-594/12, EU:C:2014:238.

53 Arrêt de la Cour du 6 octobre 2015, *Schrems,* C-362/14, EU:C:2015:650.

54 Conclusions de l'Avocat général Mengozzi sur l'avis 1/15, présentées le 8 septembre 2015, EU:C:2016:656.

des accords avec des États tiers portant sur le contrôle des données financières, comme le montre l'accord conclu avec les États-Unis sur l'accès aux données financières dans le cadre du programme de surveillance du financement du terrorisme développé par les États-Unis (Terrorism Finance Tracking Program, TFTP)[55].

C. L'autonomie d'appréciation ancrée dans le cadre constitutionnel de l'Union

Cette autonomie d'appréciation tient aux progrès du droit dérivé et aux apports de la jurisprudence de la Cour de justice. Elle doit être rattachée au cadre constitutionnel de l'Union. Comme l'a souligné l'avis 2/13 c'est « dans le respect de ce cadre constitutionnel (…) que les droits fondamentaux, tels que reconnus en particulier par la Charte, doivent être interprétés et appliqués au sein de l'Union »[56]. Cette autonomie d'interprétation s'impose pour l'appréciation des objectifs poursuivis par l'action normative de l'Union ainsi que pour l'appréciation de la proportionnalité et de la nécessité des traitements des données personnelles. L'autonomie d'interprétation de la Cour participe à la définition positive des droits fondamentaux, des concepts et du champ matériel de la protection des données personnelles (1) et à l'interprétation stricte des exceptions tenant aux objectifs de sécurité et à l'encadrement croissant de l'appréciation de ces objectifs (2).

1. L'interprétation autonome des concepts et du champ matériel de la protection des données personnelles

La Cour de justice contrôle le respect par le droit dérivé des droits fondamentaux garantis par l'Union européenne, comme principes généraux du droit et sur le fondement de la Charte des droits fondamentaux. Elle veille au respect de l'obligation d'interprétation du droit dérivé conforme au respect des droits fondamentaux. Le contrôle à la lumière de la Charte porte tant sur la protection des données personnelles protégée comme droit fon-

55 V. Potvin-Solis, « La lutte contre le terrorisme et son financement », *supra* note 32.

56 Avis 2/13, *supra* note 1, point 177.

damental que sur celle des droits fondamentaux qui lui sont liés, tout particulièrement celui du respect de la vie privée qui recouvre un champ et des bénéficiaires différents. Le principe de soumission aux traités et à leurs principes constitutionnels s'impose au droit dérivé de l'Union et aux accords internationaux avec des États tiers. La directive 95/46/CE a posé des principes de protection qui valent à l'égard de « tout traitement de données à caractère personnel dès lors que les activités du responsable du traitement relèvent du champ d'application du droit communautaire »[57]. Elle s'est appliquée aux données qui font l'objet de fichiers autonomisés ou non automatisés et a défini les notions de « données personnelles »[58] et de « traitement » de telles données[59] ainsi que les principales notions sur lesquelles la protection qu'elle a établie repose[60]. Elle a exclu notamment de son champ « le traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques »[61]. Le règlement général sur la protection des données personnelles n° 2016/679/UE qui la remplace depuis le 25 mai 2018[62] précise aussi dans ses premiers articles son objet et ses objectifs, son champ d'application matériel et territorial, les définitions de ses principales notions[63] et il en est de même des directives adoptées le même jour[64].

La Cour de justice fournit une interprétation large de la notion de données personnelles, de celle de traitement[65] et du principe de non-discrimination et d'égalité de traitement[66]. Sa jurisprudence permet de préciser le champ du droit dérivé qui couvre celui de la conciliation entre les ob-

---

57 Cons. 12 de la directive 95/46/CE, *supra* note 7.
58 *Id.,* article 2, a).
59 *Ibid.*
60 *Id.,* article 2, b).
61 Cons. 12 et article 3 de la directive.
62 Règlement n° 2016/679/UE (règlement général sur la protection des données), *supra* note 11.
63 *Id.,* article 1 à 4.
64 Directive 2016/681 et directive 2016/680, *supra* note 15.
65 Pour des questions d'interprétation de ces notions, v. par ex., les renvois préjudiciels introduits par l'Augstākā tiesa le 12 juin 2017, *Buivids,* C-345/17 et par l'Oberlandesgericht Düsseldorf le 26 janvier 2017, *Fashion ID,* C-40/17.
66 Dans son avis 1/15, *supra* note 2, la Cour considère que la compatibilité de l'accord entre le Canada et l'Union sur le transfert et le traitement de données PNR avec les articles 7, 8 et l'article 52, paragraphe 1, de la Charte des droits fondamentaux exige notamment que cet accord prévoie « que les modèles et les critères

jectifs de sécurité nationale d'une part, et la garantie des droits fondamentaux et de la protection des données personnelles, d'autre part. La Cour a notamment interprété la directive 95/46/CE par référence à la Charte des droits fondamentaux de l'Union[67] en soulignant la mention expresse dans ses dispositions du respect des droits fondamentaux et la définition même de son objet dans son article 1er[68]. Elle relève de façon constante que « la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci »[69]. Elle interprète de façon large l'objectif de la directive 95/46/CE[70] et son champ d'application territorial[71].

2. L'encadrement croissant des objectifs sécuritaires justifiant le traitement des données personnelles

La directive 95/46/CE prenait en compte les objectifs de sécurité dans les limites posées à son champ d'application et dans la portée des droits garantis. Son article 3 excluait de son champ d'application les traitements de données à caractère personnel « mis en œuvre pour l'exercice d'activ-

---

utilisés dans le cadre du traitement automatisé des données des dossiers passagers seront spécifiques et fiables ainsi que non discriminatoires ».

67 V. not. : Arrêt de la Cour du 6 mars 2001, *Connolly/Commission,* C-274/99 P, EU:C:2001:127, point 37; arrêt de la Cour du 20 mai 2003, *Österreichischer Rundfunk e.a.,* C-465/00, EU:C:2003:294, point 68; arrêt de la Cour du 13 mai 2014, *Google Spain et Google, supra* note 10, point 68; arrêt de la Cour du 11 décembre 2014, *Ryneš,* C-212/13, ECLI :EU:C:2014:2428, point 29; arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, point 38.

68 V. arrêt de la Cour du 7 mai 2009, *Rijkeboer, supra* note 8*,* points 46-47; arrêt de la Cour du 20 mai 2003, *Österreichischer Rundfunk e.a., supra* note 67, point 70; arrêt de la Cour du 6 novembre 2003, *Lindqvist, supra* note 8, points 97 et 99; arrêt de la Cour du 29 janvier 2008, *Promusicae, supra* note 39, point 63; arrêt de la Cour du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia,* C-73/07, EU:C:2008:727, point 52.

69 Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a., supra* note 52, point 53.

70 V. arrêt de la Cour du 13 mai 2014, *Google Spain et Google, supra* note 10, point 53, citant par analogie, l'arrêt de la Cour du 12 juillet 2011, *L'Oréal e.a.,* C-324/09, EU:C:2011:474, points 62 et 63.

71 V. arrêt de la Cour du 13 mai 2014, *Google Spain et Google, supra* note 10, point 54.

ités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne », et, « en tout état de cause », les traitements « ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal »[72]. Elle ajoutait qu'elle ne préjugeait pas « des règles de territorialité applicables en matière de droit pénal »[73]. Elle précisait les motifs légitimes de limitation par les États, dans le respect du principe de légalité et de proportionnalité, des droits et obligations qu'elle posait [74] et fixait, dans son article 7, les principes relatifs à la légitimation des traitements de données. La Cour de justice a interprété cet article comme permettant le traitement de données à caractère personnel « lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les libertés et les droits fondamentaux de la personne concernée, notamment son droit au respect de sa vie privée à l'égard du traitement des données à caractère personnel, qui appellent une protection au titre de l'article 1er, paragraphe 1, de cette directive ». Selon la Cour de justice, l'application de cette disposition « nécessite ainsi une pondération des droits et des intérêts opposés en cause dans le cadre de laquelle il doit être tenu compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la Charte »[75]. De même, la Cour de justice encadre de façon stricte les limitations à la protection des données personnelles et le champ des exceptions prévues par la directive

---

72 V. aussi les considérant 13 et 16 de la directive 95/46/CE, *supra* note 7.

73 *Id.,* considérant 21.

74 Article 13 de la directive qui vise : « a) la sûreté de l'État; b) la défense; c) la sécurité publique; d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées; e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal; f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e); g) la protection de la personne concernée ou des droits et libertés d'autrui ».

75 Arrêt de la Cour du 13 mai 2014, *Google Spain et Google, supra* note 10, point 74, qui renvoie à l'arrêt de la Cour du 24 novembre 2011, *ASNEF et FECEMD,* C-468/10 et C-469/10, ECLI/EU:C:2011:777, points 38 et 40.

95/46/CE. Dans l'arrêt *Institut professionnel des agents immobiliers* elle rappelle sa jurisprudence constante, selon laquelle « la protection du droit fondamental à la vie privée exige que les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire »[76].

Le règlement général sur la protection des données personnelles qui remplace la directive 95/46/CE fixe le même ordre de restrictions à son champ d'application et de motifs légitimes pouvant limiter les droits et obligations qu'il pose. Son article 2, paragraphe 2, exclut de son champ d'application les traitements effectués : « a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union; b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne; c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique; d) 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, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces ». Il reprend, dans son article 23, en les complétant, les motifs légitimes pouvant justifier des limitations aux droits et obligations qu'il pose[77].

---

76 Arrêt de la Cour du 7 novembre 2013, *Institut professionnel des agents immobiliers* (*IPI*), *supra* note 38, point 39, se référant aux arrêts du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, *supra* note 68, point 56, et arrêt de la Cour du 9 novembre 2010, *Volker und Markus Schecke et Eifert,* C-92/09 et C-93/09, EU:C:2010:662, points 77 et 86.

77 « a) la sécurité nationale; b) la défense nationale; c) la sécurité publique; d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale; f) la protection de l'indépendance de la justice et des procédures judiciaires; g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière; h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g); i) la protection de la personne concernée ou des droits et libertés d'autrui; j) l'exécution des demandes de droit civil ».

II. Les progrès de l'identité européenne par l'affirmation d'un système constitutionnel de protection propre à l'Union

C'est par l'autonomie d'un tel système, de nature constitutionnelle, que peut être assurée la maîtrise par l'Union de la conciliation des intérêts. Cette autonomie s'observe dans la jurisprudence de la Cour de justice qui fait apparaître tant les jeux d'influences avec la jurisprudence de la Cour européenne des droits de l'homme que le progrès de l'autonomie du droit de l'Union dans la garantie des droits fondamentaux et les avancées spécifiques à la protection des données personnelles. L'impératif d'un tel système, d'ordre constitutionnel et qui appartienne en propre à l'Union, s'impose à bien des égards : pour fonder sur des bases solides l'articulation entre les dimensions interne et externe de la protection des données personnelles par l'Union; pour déterminer, dans le respect des principes de cohérence et de proportionnalité, la conciliation entre la protection des données personnelles, la libre circulation de ces données et les objectifs de sécurité poursuivis tant par les États membres que par l'Union; pour identifier la base juridique fondant l'activité normative et décisionnelle de l'Union en fonction des politiques en présence et des objectifs poursuivis. Les traits d'un tel système se trouvent progressivement affinés par la double portée interne et externe des progrès du contrôle juridictionnel (A) et par la portée transversale de l'exigence d'indépendance des autorités de contrôle (B) qui participent à la singularité croissante du système de protection de l'Union (C).

A. La double portée interne et externe des progrès du contrôle juridictionnel

La jurisprudence de la Cour de justice précise les conditions d'appréciation de la proportionnalité qu'elle lie au cadre constitutionnel de l'Union et qui exigent, on l'a vu, un rapport de stricte proportionnalité. Elle contribue à l'identification de l'essentiel des droits fondamentaux garanti par la Charte tant au regard de leur substance matérielle que du point de vue de leur garantie procédurale. Elle permet une interprétation évolutive de la protection des données personnelles et des droits qui entrent dans ce champ tout en montrant qu'ils ne constituent pas des prérogatives absolues. Il s'agit d'une jurisprudence dynamique qui contribue aux avancées matérielles de la substance des droits fondamentaux et des

éléments essentiels de la protection des données personnelles (1) et qui rapporte le contrôle de stricte proportionnalité à l'exigence de clarté et de précision qui s'impose à l'encadrement légal des ingérences (2).

1. *Les avancées matérielles de la substance des droits fondamentaux et des éléments essentiels de la protection des données personnelles*

Les progrès du droit dérivé peuvent amener ces avancées matérielles et font alors l'objet d'une interprétation extensive de la part de la Cour de justice. Ainsi, la directive 95/46/CE a énoncé les garanties des personnes concernées par le traitement des données personnelles en termes de qualité et d'exactitude des données, qui doivent être traitées loyalement et licitement, et être collectées pour des finalités déterminées, explicites et légitimes. Elle a exigé le consentement de la personne[78] en prévoyant les hypothèses dans lesquelles celui-ci peut être limité lorsque le traitement des données est nécessaire pour la poursuite d'intérêts légitimes définis. Elle a précisé les catégories de traitements interdits, en particulier ceux qui portent sur des données sensibles « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle »[79]. Elle a énoncé les droits des personnes concernées en matière d'information[80], d'accès[81], d'opposition[82], de confidentialité et de sécurité des traitements[83], de notification, de contrôle préalable et de publicité des traitements[84] et de recours, de responsabilité et de sanctions en cas de non-respect des dispositions prises pour son application[85]. La jurisprudence a fixé l'étendue des bénéficiaires de la protection des données personnelles qui vaut à l'égard des personnes physiques mais non à l'égard des personnes morales[86] ainsi que l'articula-

78 Articles 6 et 7 de la directive 95/46/CE, *supra* note 7.
79 *Id.,* Article 8-1.
80 *Id.,* Articles 10 et 11.
81 *Id.,* Article 12.
82 *Id.,* Articles 14 et 15.
83 *Id.,* Articles 16 et 17.
84 *Id.,* Articles 18 à 21.
85 *Id.,* Articles 22 à 24.
86 Arrêt de la Cour du 17 décembre 2015, *WebMindLicenses,* C-419/14, EU:C:2015:832, point 79.

tion entre l'article 8 CDFUE et l'article 7 CDFUE qui est quant à lui applicable à ces dernières[87].

Dans l'arrêt *Google Spain*[88], la Cour de justice se prononce sur la responsabilité de l'exploitant d'un moteur de recherches sur internet pour le traitement qu'il effectue des données à caractère personnel apparaissant sur des pages web publiées par des tiers. La Cour souligne la facilité d'accéder à une multitude d'aspects de la vie privée par des moteurs de recherches et la possibilité d'établir un profil plus ou moins détaillé de la personne recherchée ainsi que l'ingérence qui en résulte dans les droits de la personne recherchée. Elle met en avant l'intérêt légitime des internautes à avoir accès à des informations concernant une personne déterminée. Mais elle recherche, en même temps, le juste équilibre entre cet intérêt des utilisateurs des réseaux internet et les droits fondamentaux des personnes concernées. De plus, elle relève que le traitement licite de données exactes « peut se transformer dans le temps et devenir incompatible avec la directive 95/46/CE si au regard des circonstances elles apparaissent inadéquates, pas ou plus pertinentes, ou excessives au regard des finalités pour lesquelles elles ont été traitées et du temps qui s'est écoulé ». La Cour pose ainsi une jurisprudence créatrice en reconnaissant le droit à l'effacement et à la suppression des liens vers les pages web contenant des informations sur des données d'une personne[89] avec une exception tenant à la prise en compte du rôle de la personne concernée dans la vie publique justifiant un intérêt prépondérant du public à accéder à ces informations.

Les apports matériels de la jurisprudence de la Cour de justice tiennent aussi à ce qu'elle permet de préciser les contours des éléments essentiels de la protection des données personnelles et des droits fondamentaux œuvrant dans ce champ. Ont par exemple été considérées comme portant atteinte à ces éléments essentiels : la possibilité laissée aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques (portant atteinte aux éléments essentiels du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la

87 *Id.,* point 80.

88 Arrêt de la Cour du 13 mai 2014, *Google Spain et Google*, *supra* note 10.

89 V. la demande de décision préjudicielle présentée par le Conseil d'État français le 21 août 2017, *Google Inc. / Commission nationale de l'informatique et des libertés (CNIL),* C-507/17, qui vise à ce que la Cour de justice précise la portée du « droit au déréférencement » consacré par l'arrêt *Google Spain* et l'étendue des obligations qu'il engendre pour l'exploitant d'un moteur de recherche.

Charte)[90]; l'absence de voie de droit ouverte au justiciable permettant d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de celles-ci (portant atteinte aux éléments essentiels du droit à une protection juridictionnelle effective garanti par l'article 47 de la Charte)[91]. Le droit à un contrôle par des autorités indépendantes est aussi considéré comme « un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel »[92].

2. *Le contrôle strict de proportionnalité et l'exigence de clarté et de précision de l'encadrement légal des ingérences*

La Cour de justice applique un contrôle strict du respect des conditions de proportionnalité des ingérences dans le droit à la protection des données personnelles. Elle encadre la marge d'appréciation du législateur de l'Union et exige que la base légale définisse elle-même la portée des limitations qu'elle prévoit à la protection des données personnelles. En se référant notamment à la jurisprudence de la Cour européenne des droits de l'homme, elle relève que « l'exigence que toute limitation de l'exercice de ce droit doit être prévue par la loi implique que la base légale (…) doit être suffisamment claire et précise et que, en définissant elle-même la portée de la limitation de l'exercice du droit garanti par l'article 7 de la Charte, elle offre une certaine protection contre d'éventuelles atteintes arbitraires de cette administration »[93]. Pour reprendre les termes de ses arrêts, « en ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi

90 Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a., supra* note 52, point 39 et arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, point 94.

91 Arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, point 95.

92 *Id.*, point 41 et point 68 renvoyant notamment à l'arrêt de la Cour du 16 octobre 2012, *Commission/Autriche*, C-614/10, EU:C:2012:631.

93 Arrêt de la Cour du 17 décembre 2015, *WebMindLicenses, supra* note 86, point 81, qui renvoie aux arrêts de la Cour EDH, du 2 août 1984, *Malone/Royaume-Uni,* paragraphe 67, et du 12 janvier 2010, *Gillan et Quinton/Royaume-Uni,* paragraphe 77.

lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci»[94]. Le CEPD rappelle régulièrement les exigences du principe de proportionnalité dans la jurisprudence de la Cour de justice. Cette jurisprudence impose un encadrement par des règles claires et précises des ingérences dans le droit à la protection des données personnelles tant à l'égard du droit dérivé de l'Union que des accords internationaux avec des États tiers. Dans l'arrêt *Digital Rights Irelands*[95]*,* la Cour de justice déclare invalide la directive 2006/24/CE[96]. Elle constate « une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel » qui n'est pas limitée au strict nécessaire. Elle rappelle que « la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »[97]. Tel n'était pas le cas des dispositions de la directive 2006/24/CE qui est par conséquent jugée invalide[98].

La Cour de justice encadre également le renvoi au droit des États membres pour la définition des infractions graves justifiant le traitement de données personnelles. Les mêmes exigences s'imposent dans les relations avec les États tiers[99] et les accords internationaux relatifs aux transferts de données personnelles doivent prévoir des ingérences limitées au strict nécessaire et comporter des règles claires et précises au regard tant des données à transférer que de l'encadrement de la portée de l'ingérence dans

94 Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a., supra* note 52.

95 *Ibid.*

96 Directive 2006/24/CE du Parlement européen 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, *JO* L 105, du 13 avril 2016, p. 54.

97 Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a., supra* note 52*,* point 54. La Cour applique ici une interprétation par analogie de la jurisprudence de la Cour EDH relative à l'article 8 de la CEDH.

98 *Id.,* point 65.

99 Arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, points 91 et s.

les droits fondamentaux[100]. De tels accords sont ainsi appréciés à l'aune de l'exigence de clarté et de précision telle qu'elle est entendue et appliquée par la Cour de justice.

B. La portée transversale de l'exigence d'indépendance des autorités de contrôle

Le paragraphe 2 de l'article 16 TFUE vise tant « les institutions, organes et organismes de l'Union » que « les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union ». Les termes de cette obligation d'indépendance sont définis par le droit de l'Union européenne dans son champ de protection et tiennent à la liaison et à l'interdépendance entre les ordres juridiques. Il en est ainsi tout particulièrement de l'exigence d'indépendance des autorités de contrôle du respect des règles relatives à la protection des données personnelles qui est expressément posée aux articles 16 TFUE, 39 TUE et 8 CDFUE. Il s'agit d'une obligation opposable tant aux États qu'à l'Union (1) et qui fait l'objet d'une interprétation large par l'autonomie du concept d'indépendance et ses prolongements externes (2).

1. Une obligation opposable aux États membres et à l'Union aux plans interne et externe

L'indépendance est imposée à toute autorité, européenne et nationale, de contrôle du respect du droit à la protection des données personnelles, par le paragraphe 3 de l'article 8 de la Charte des droits fondamentaux de l'Union. À l'égard des États membres, le considérant 62 de la directive 95/46/CE soulignait que « l'institution, dans les États membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel ». Cette exigence faisait l'objet de l'article 28 de la directive 95/46/CE[101]. Elle est confortée par le règlement général sur la protection des données personnelles n° 2016/679/UE et est

100 Avis de la Cour du 26 juillet 2017, 1/15, *supra* note 2.

101 Selon les paragraphes 1 et 2 de cet article : « 1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application,

également posée par le règlement n° 45/2001/CE qui prévoit notamment l'établissement d'une instance de surveillance indépendante chargée de contrôler l'application de ses dispositions. La Cour de justice peut être amenée à statuer sur le respect de cette exigence. Dans l'arrêt *Commission/Allemagne,* elle juge que l'Allemagne n'a pas respecté les exigences du paragraphe 1 de l'article 28 de la directive 95/46/CE, « en soumettant à la tutelle de l'État les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel par le secteur non public dans les différents Länder » [102]. Dans l'arrêt *Commission/Autriche*[103], elle se prononce dans le même sens en jugeant que l'Autriche n'a pas pris « toutes les dispositions nécessaires » pour satisfaire au critère d'indépendance concernant la Datenschutzkommission (commission de protection des données, ci-après la «DSK»), instituée en tant qu'autorité de contrôle de la protection des données à caractère personnel »[104]. Puis, dans l'arrêt *Commission/Hongrie*[105], la Cour condamne la décision du gouvernement hongrois de mettre fin brutalement aux fonctions du Commissaire hongrois à la protection des données. Elle insiste sur la nécessaire indépendance des autorités qui dans les États sont chargées de veiller au respect de la directive 95/46/CE. Elle souligne que « l'exigence de contrôle par une autorité indépendante du respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel résulte également du droit primaire de l'Union, notamment de l'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne et de l'article 16, paragraphe 2,

---

sur son territoire, des dispositions adoptées par les États membres en application de la présente directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies. 2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel ».

102 Arrêt de la Cour du 9 mars 2010, *Commission/Allemagne,* C-518/07, EU:C:2010:125, point 56.

103 Arrêt de la Cour du 16 octobre 2012, *Commission/Autriche, supra* note 92.

104 *Id.,* point 66, précisant que, selon le cadre réglementaire autrichien : « – le membre administrateur de la DSK est un fonctionnaire fédéral assujetti à une tutelle de service; -le bureau de la DSK est intégré aux services de la chancellerie fédérale, et – le chancelier fédéral dispose d'un droit inconditionnel à l'information sur tous les aspects de la gestion de la DSK ».

105 Arrêt de la Cour du 8 avril 2014, *Commission/Hongrie,* C-288/12, EU:C:2014:237.

TFUE »[106]. Elle rappelle à cette occasion sa jurisprudence selon laquelle « l'institution, dans les États membres, d'autorités de contrôle indépendantes constitue ainsi un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel »[107], « comme cela est d'ailleurs relevé au considérant 62 de la directive 95/46 ». Elle juge qu' « en mettant fin de manière anticipée au mandat de l'autorité de contrôle de la protection des données à caractère personnel, la Hongrie a manqué aux obligations qui lui incombent en vertu de la directive 95/46/CE 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 ».

La directive 95/46/CE prévoyait l'institution d'un groupe de protection des personnes à l'égard du traitement des données à caractère personnel composé de représentants des autorités de contrôle national, de représentants des autorités de contrôle des institutions et organismes de l'Union et d'un représentant de la Commission européenne. Le règlement n° 45/2001/CE relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et à la libre circulation des données prévoit l'établissement d'une instance de surveillance indépendante chargée de contrôler l'application de ses dispositions. Selon son considérant 2, « un système à part entière de protection des données à caractère personnel impose non seulement de conférer des droits aux personnes concernées et des obligations à celles qui traitent des données à caractère personnel, mais aussi de prévoir des sanctions appropriées pour les contrevenants ainsi qu'une autorité de contrôle indépendante »[108]. Ce règlement institue, pour le contrôle de l'application de ses dispositions « à tous les traitements effectués par une institution ou un organe communautaire », une « autorité de contrôle indépendante », le « contrôleur européen de la protection des données »[109]. Enfin, le règlement général sur la protection des données

106 *Id.,* point 48.

107 Point 48 citant l'arrêt de la Cour du 9 mars 2010, *Commission/Allemagne, supra* note 102, point 23, et l'arrêt de la Cour du 16 octobre 2012, *Commission/Autriche, supra* note 92, point 37.

108 Règlement n° 45/2001/CE, *supra* note 16.

109 *Id.,* article 1, paragraphe 2.

personnelles 2016/679/UE, qui remplace la directive 95/46/CE,[110] prévoit l'institution dans les États membres d'un délégué à la protection des données[111] et consacre son chapitre VI aux autorités de contrôle indépendantes. Les mêmes dispositions sont reprises dans la directive 2016/680/UE dans le domaine de la coopération en matière pénale[112].

2. L'autonomie du concept d'indépendance dans la jurisprudence et ses prolongements externes

La Cour de justice a adopté une conception large de la notion d'indépendance en précisant qu'elle respecte, ce faisant, la répartition des compétences entre l'Union et ses États membres. Selon la Cour de justice : « La garantie d'indépendance des autorités nationales de contrôle vise à assurer l'efficacité et la fiabilité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel et doit être interprétée à la lumière de cet objectif. Elle a été établie en vue de renforcer la protection des personnes et des organismes qui sont concernés par les décisions de ces autorités »[113]. La notion d'indépendance est définie comme une notion autonome et largement entendue par l'arrêt *Commission/Allemagne*[114]. Cet arrêt situe l'exigence d'indépendance dans le contexte plus large de la protection des droits fondamentaux, de la protection de la vie privée et du principe de démocratie. Il se réfère à la jurisprudence de la Cour européenne des droits de l'homme pour dégager une vision systémique de cette indépendance telle qu'elle s'impose dans l'ordre juridique de l'Union. Il écarte l'argumentation selon laquelle l'interprétation large de la notion d'indépendance dépasse les limites de la compétence de l'Union. Selon les arrêts *Commission/Allemagne*, *Commission/Autriche* et *Commission/Hongrie*, la notion d'indépendance « exclut notamment toute injonction et toute autre influence extérieure sous quelque forme que ce soit,

110 Règlement n° 2016/679/UE (règlement général sur la protection des données), *supra* note 11.

111 Articles 37 à 39 du règlement.

112 Directive 2016/680/UE, *supra* note 15; v. les articles 32 à 34 de la directive relatifs à l'institution dans les États membres d'un délégué à la protection des données et son chapitre VI relatif aux autorités de contrôle indépendantes.

113 Arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, point 41.

114 Arrêt de la Cour du 9 mars 2010, *Commission/Allemagne, supra* note 102.

qu'elle soit directe ou indirecte, qui seraient susceptibles d'orienter leurs décisions et qui pourraient ainsi remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel »[115]. La Cour impose une indépendance fonctionnelle et exige que l'autorité puisse être « considérée comme pouvant opérer, en toute circonstance, au-dessus de tout soupçon de partialité »[116]. Cette lecture rejoint la conception de l'indépendance et de l'impartialité développée par la jurisprudence de Strasbourg qui fait intervenir un double critère objectif et subjectif. La Cour de justice a également été amenée à opérer un raisonnement par analogie dans l'interprétation des exigences d'indépendance au sens du règlement n° 45/2001/CE[117].

Dans l'arrêt *Digital Rights Ireland*, la Cour de justice a relevé que la directive 2006/24/CE 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, « n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité »[118]. De même, la Cour a exercé son contrôle, dans l'arrêt *Schrems,* sur la décision de la Commission constatant l'adéquation de la protection des données personnelles dans un État tiers, en soulignant que cette dernière n'a pas compétence pour « restreindre les pouvoirs des autorités nationales de contrôle »[119]. Dans l'arrêt, *Tele2 Sverige*, elle a inter-

115 V. l'arrêt de la Cour du 9 mars 2010, *Commission/Allemagne, supra* note 102, point 30, l'arrêt de la Cour du 16 octobre 2012, *Commission/Autriche, supra* note 92*,* points 41 et 43 et l'arrêt de la Cour du 8 avril 2014, *Commission/Hongrie, supra* note 105*,* point 51.

116 V. l'arrêt de la Cour du 8 avril 2014, *Commission/Hongrie, supra* note 105*,* point 55 qui en conclut notamment que « l'exigence d'indépendance figurant à l'article 28, paragraphe 1, second alinéa, de la directive 95/46 doit, dès lors, nécessairement être interprétée comme incluant l'obligation de respecter la durée du mandat des autorités de contrôle jusqu'à son échéance et de n'y mettre fin de manière anticipée que dans le respect des règles et des garanties de la législation applicable ».

117 *Id.,* points 56 et s.

118 Point 68 renvoyant notamment à l'arrêt de la Cour du 16 octobre 2012, *Commission/Autriche, supra* note 92*,* point 37.

119 Arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, points 99 à 104.

prété l'article 15, paragraphe 1, de la directive 2002/58, par référence aux articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux, pour juger que cette disposition « s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union »[120]. Ainsi, dans l'avis 1/15, la Cour de justice a exigé que l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers garantisse que « la surveillance des règles » qu'il prévoit pour la protection des passagers aériens à l'égard du traitement des données des dossiers passagers les concernant, soit « assurée par une autorité de contrôle indépendante »[121].

C. La singularité croissante du système de protection des données personnelles par l'Union

La conciliation entre l'objectif de protection des données personnelles et l'objectif de sécurité implique des précisions sur la répartition des compétences entre l'Union et ses États membres et sur le choix de la base juridique des actes de l'Union. Il en est ainsi même dans le contexte des relations externes avec des États tiers. L'imbrication entre les objectifs internes et externes agit sur l'articulation des bases juridiques et des compétences en fonction des objectifs poursuivis (1). Elle invite à l'affirmation d'une identité de l'Union qui progresse notamment par la continuité imposée entre la protection substantiellement équivalente établie par référence à un niveau élevé de protection dans l'Union et la protection adéquate exigée des État tiers (2).

120 Arrêt de la Cour du 21 décembre 2016, *supra* note 24.
121 Avis de la Cour du 26 juillet 2017, 1/15, *supra* note 2.

1. *L'imbrication entre les objectifs internes et externes et l'articulation des bases juridiques et des compétences*

La conciliation entre la protection des données personnelles et les autres objectifs du droit de l'Union se pose en termes d'articulation des bases juridiques. La Cour de justice rappelle de façon constante que le choix de la base juridique d'un acte de l'Union doit reposer « sur des éléments objectifs susceptibles de contrôle juridictionnel, parmi lesquels figurent la finalité et le contenu de cet acte »[122]. Il peut conduire à déterminer la finalité prépondérante de l'acte ou de l'accord international en présence ou à retenir une double base juridique en cas de finalités indissociables de l'une de l'autre et d'absence d'incompatibilité entre les procédures auxquelles elles renvoient respectivement. Les termes de la conciliation entre les objectifs de protection des données personnelles et de sécurité peuvent donc impliquer de rechercher quel est l'objectif dominant pour déterminer la base juridique. De plus, la délimitation du domaine des exceptions prévues par les actes du droit dérivé à leur champ d'application, notamment pour la préservation d'objectifs de sécurité, agit sur la détermination des bases juridiques. Ainsi, dans l'arrêt *Parlement/Conseil et Commission*, la Cour relève que la décision 2004/535/CE de la Commission, qui était en cause dans cette affaire avait trait au transfert des données des passagers provenant des systèmes de réservation des transporteurs aériens situés sur le territoire des États membres au Bureau des douanes et de la protection des frontières du ministère de la Sécurité intérieure des États-Unis. Elle souligne que ce traitement de données « n'était pas nécessaire à la réalisation d'une prestation de services par les transporteurs aériens », mais était considéré comme tel « pour sauvegarder la sécurité publique et à des fins répressives ». Ce traitement relevait donc de l'article 3, paragraphe 2, de la directive 95/46/CE[123]. Elle en conclut que la décision de conclusion de l'accord ne relevait pas du champ d'application de la direc-

122 V. notamment l'avis de la Cour du 26 juillet 2017, 1/15, *supra* note 2, points 76 et s.

123 Excluant de son champ « les traitements de données personnelles ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal » (v. nos développements *supra*), arrêt de la Cour du 30 mai 2006, *Parlement/Conseil et Commission*, *supra* note 50, points 57 à 59.

tive 95/46/CE et ne pouvait donc pas être fondée sur l'article 95 CE[124]. Dans l'arrêt *Irlande/Parlement et Conseil,* la Cour refuse de transposer ce raisonnement à la directive 2006/24/CE (communications électroniques)[125]. Elle souligne qu' « à la différence de la décision 2004/496/UE, qui concernait un transfert de données personnelles s'insérant dans un cadre institué par les pouvoirs publics en vue d'assurer la sécurité publique, la directive 2006/24/CE vise les activités des fournisseurs de services dans le marché intérieur et ne comporte aucune réglementation des activités des pouvoirs publics à des fins répressives ». Elle en conclut que l'adoption de la directive 2006/24/CE sur la base de l'article 95 CE s'imposait.

Dans son avis 1/15, la Cour rappelle la méthode de détermination des bases juridiques en soulignant que cette question revêt une « importance de nature constitutionnelle »[126] et que « le recours à une base juridique erronée est susceptible d'invalider l'acte de conclusion lui-même et, partant, de vicier le consentement de l'Union à être liée par l'accord auquel cette dernière a souscrit »[127]. La Cour se prononce en faveur du double fondement car le projet d'accord PNR possède « une double composante, l'une concernant la nécessité d'assurer la sécurité publique et l'autre concernant la protection des données PNR » et car ses deux composantes « sont liées de façon indissociable » et « doivent donc être considérées toutes les deux comme présentant un caractère essentiel »[128]. La Cour en conclut que la décision de conclusion de l'accord PNR projeté entre l'Union et le Canada doit être fondée conjointement sur l'article 16, paragraphe 2, et sur l'article 87, paragraphe 2, sous a), TFUE, après avoir statué dans le sens de la compatibilité entre leurs procédures respectives[129].

---

124 L'arrêt en conclut que « l'article 95 CE, lu en combinaison avec l'article 25 de la directive, n'est pas susceptible de fonder la compétence de la Communauté pour conclure l'accord ». Arrêt de la Cour du 30 mai 2006, *Parlement/Conseil et Commission*, *supra* note 50, points 68 et 69.

125 Arrêt du 10 février 2009, C-301/06, *Parlement/Conseil et Commission,* EU:C:2009:68.

126 Point 71 de l'avis 1/15, *supra* note 2, renvoyant à l'arrêt de la Cour du 1er octobre 2009, *Commission/Conseil*, C-370/07, EU:C:2009:590, point 47.

127 Point 72 de l'avis 1/15, *supra* note 2.

128 *Id.,* points 90 et 94.

129 *Id.,* point 105 et s. Dans ses conclusions sur l'avis 1/15 (*supra* note 54) l'Avocat général Paolo Mengozzi proposait à la Cour de juger que l'accord devait être

2. *L'identité de l'Union par la continuité entre la protection substantiellement équivalente visant un niveau élevé de protection et la protection adéquate exigée des États tiers*

L'exigence d'une protection adéquate s'impose dans les rapports avec les États tiers et est appréciée dans ce contexte externe par référence aux exigences internes à l'Union. Si la protection adéquate ne renvoie pas à une protection identique, elle tend à être alignée par la Cour de justice sur le niveau élevé de protection recherché dans l'Union. Le niveau de protection adéquate rejoint ainsi le niveau de protection élevé par référence à celui applicable en interne à l'Union. La Cour de justice peut ainsi être amenée à contrôler le caractère adéquat du niveau de protection assuré par les États tiers avec lesquels l'Union entend procéder à des transferts de données personnelles. Elle a ainsi jugé dans l'arrêt *Schrems* que l'intervention d'une décision de la Commission européenne constatant le caractère adéquat du niveau de protection dans un pays tiers « ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, telle que modifiée, examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat »[130]. Comme le montre cet arrêt, le contrôle exercé à l'égard de l'État tiers n'est que le pendant du niveau de protection défini en interne à l'Union. Il s'agit d'éviter que l'État membre puisse contourner le niveau de protection exigé dans l'Union en procédant par des transferts de données personnelles vers des États tiers pour leur traitement dans ces États[131].

Le niveau de protection adéquate est interprété par la Cour de justice par référence au droit dérivé « lu à la lumière de la Charte ». Il exige que le pays tiers « assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46/CE, lue à la lumière de la

---

basé tant sur l'article 16 paragraphe 2, alinéa 1, TFUE que sur l'article 87 paragraphe 2, a) TFUE.

130 Arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53, point 38.

131 *Id.,* point 73.

Charte » avec des moyens qui « doivent néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union »[132]. La Cour applique ce raisonnement dans l'avis 1/15, dans lequel elle rappelle fermement les conditions d'appréciation et les exigences constitutionnelles qui gouvernement l'étendue de son contrôle juridictionnel. En premier lieu, « l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné ». En second lieu, le respect du principe de proportionnalité implique que « les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire » et « pour satisfaire à cette exigence, la réglementation en cause comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus »[133].

L'appréciation de la protection adéquate comporte donc celle de l'encadrement légal par des règles claires et précises des ingérences dans les droits fondamentaux justifiées par des raisons de sécurité dans l'État tiers[134]. Elle s'impose à la Commission lorsqu'elle se prononce sur le niveau d'adéquation de la protection assurée dans un État tiers. Ainsi, dans l'arrêt *Schrems,* la Cour relève que la décision de la Commission constatant que les États-Unis assurent un niveau de protection adéquat, « ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale » et qu'elle « ne fait pas état de l'existence d'une protection juridique efficace contre des

132 *Id.*, points 73 et 74.

133 Avis de la Cour du 26 juillet 2017, 1/15, *supra* note 2; v. Potvin-Solis « La lutte contre le terrorisme et son financement », *supra* note 30.

134 Arrêt de la Cour du 6 octobre 2015, *Schrems, supra* note 53,point 87.

ingérences de cette nature »[135]. L'avis 1/15 rappelle fermement le contrôle strict qu'entend opérer la Cour de justice pour assurer la garantie des droits fondamentaux et du droit à la protection des données personnelles par les accords internationaux conclus par l'Union pour le traitement et le transfert des telles données. Il poursuit ainsi dans la voie d'une affirmation grandissante de l'autonomie du système de protection et de l'identité constitutionnelle de l'Union européenne dans cette garantie face aux objectifs de sécurité.

135 *Id.*, points 88 et 89.