RTD Eur. 2015 p.117

La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel

(CJUE 8 avr. 2014, aff. jtes C-293/12 et C-594/12, *Digital Rights Ireland Ltd*, AJDA 2014. 773 ; *ibid*. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1355, et les obs. , note C. Castets-Renard ; *ibid*. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny)

Sylvie Peyrou, Maître de conférences, Université de Pau et des Pays de l'Adour, CDRE Bayonne

*
**

« La Charte des droits fondamentaux n'est pas un tigre de papier » (1), la Cour de justice de l'Union européenne (CJUE) vient de le démontrer avec éclat dans un arrêt promis à figurer parmi les grands (2). C'est la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006, sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, qui se trouve ici sur la sellette. Ce texte a fait couler beaucoup d'encre au sein de diverses juridictions constitutionnelles européennes (3) et a déjà été soumis au demeurant à l'examen de la Cour de justice par un recours en annulation sous l'angle de sa base légale (4). Il lui est à nouveau présenté, par la voie préjudicielle cette fois, afin qu'elle se prononce sur la question de sa validité. Deux demandes lui sont adressées, l'une par la Haute Cour irlandaise *(High Court)*, saisie d'un litige par l'ONG *Digital Rights Ireland* (5) au sujet de la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques, et l'autre par la Cour constitutionnelle autrichienne *(Verfassungsgerichtshof)*, suite aux recours constitutionnels introduits auprès d'elle à la fois par le gouvernement du Land de Carinthie *(Kärntner Landesregierung)* et par MM. Seitlinger, Tschohl et plus de onze mille autres requérants, au sujet de la conformité à la Constitution fédérale *(Bundes-Verfassungsgesetz)* de la loi de transposition de la directive.

Dans le contexte de l'après 11 septembre 2001, la directive de 2006, organisant la « rétention des données » de connexion par les opérateurs de télécommunications ou les fournisseurs d'accès à internet, est « l'une des législations-clés de l'Union en matière de lutte anti-terrorisme » (6). Elle impose ainsi aux fournisseurs de services de conserver, pour une durée de six mois à deux ans, tout un ensemble de données permettant d'identifier l'émetteur et le destinataire d'une communication, la durée de celle-ci, sa localisation, etc., afin de permettre aux autorités nationales d'y accéder dans le cadre de la lutte contre le terrorisme ou la criminalité grave. Mais le nombre et la nature des données ainsi recueillies font problème, dès lors qu'elles permettent de dessiner une « cartographie aussi fidèle qu'exhaustive [...] des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée », comme le relève l'avocat général Cruz Villalon dans des conclusions très sévères (7).

C'est donc sous l'angle du respect des droits fondamentaux qu'est posée à la Cour de justice la question de la validité de la directive, plus précisément du droit au respect de la vie privée et de celui à la protection des données à caractère personnel, garantis respectivement par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (8). Elle y répond sans détour, par un arrêt prononçant l'invalidité de la directive dans son intégralité et *ab initio*, solution rarissime et radicale (au contraire de celle, mesurée, préconisée par l'avocat général (9)) obligeant le législateur à revoir sa copie sans délai. L'arrêt est ainsi d'importance, tant dans son raisonnement que dans ses conclusions : « À une question de principe, la Cour apporte sans se dérober une réponse de même nature » (10).

Il est vrai que le contexte, tant politique que juridique, y était favorable. Ainsi, d'abord, les révélations d'E. Snowden (11) ont sans doute joué un grand rôle, apprenant à une opinion médusée (12) que, par le biais du système « Prism », la NSA *(National Security Agency)* et le FBI *(Federal Bureau of Investigation)* américains avaient directement accès aux données de communications de millions de citoyens, aussi bien américains qu'européens. Cet espionnage à grande échelle, qui plus est par un allié de l'Europe, n'a pas manqué de sensibiliser tout un chacun à la question de la protection de ses données à caractère personnel. Ensuite, une Charte des droits fondamentaux de l'Union, élevée au rang de droit primaire grâce au traité de Lisbonne, s'est révélée l'instrument idéal pour la Cour afin de jauger une directive limitant manifestement les droits garantis par celle-ci. Il ne faut cependant pas s'y tromper, les droits proclamés par la Charte ne sont pas inconditionnels et - dans une logique analogue à celle de la Convention européenne des droits de l'homme (Conv. EDH) - l'article 52, paragraphe 1, de la même Charte prévoit en les encadrant les limites pouvant être apportées aux droits protégés (13). C'est donc à une analyse systématique et sans concessions que la Cour va se livrer, soumettant notamment la directive incriminée à un calcul de proportionnalité inspiré de son homologue strasbourgeoise. Mais - cet aspect méthodologique est à souligner -, la Cour axe l'ensemble de son raisonnement sur la Charte et sur elle seule, celle-ci lui fournissant à la fois sa « norme de référence » (14) et sa grille d'analyse, donnant ainsi une autonomie inédite au juge de Luxembourg.

L'ensemble de ces paramètres concourt à faire de l'arrêt rendu par la Cour de justice le 8 avril 2014 un arrêt historique. Le point majeur est bien évidemment celui relatif à la protection des données à caractère personnel, qui bénéficie d'un ancrage « constitutionnel », placé désormais sous la vigilance du juge, il le prouve ici. Mais, au-delà, on retiendra la mutation de l'Union européenne qui, à défaut de s'être dotée formellement d'un « Traité constitutionnel » (hérétique juridiquement...) a incontestablement franchi un seuil grâce au traité de Lisbonne. L'affirmation symbolique (15) et juridique (16) de ses valeurs par l'Union européenne donnent en effet par la même un nouvel élan à la Cour de justice, tout en facilitant son office. L'idée qui émerge, par-delà les arguments techniques relatifs à l'analyse de l'ingérence dans les droits garantis ou au calcul de proportionnalité, est ainsi celle d'une Charte des droits fondamentaux devenue norme de référence du contrôle opéré par la Cour de justice (**I**), permettant à celle-ci de s'affirmer en tant que juge « constitutionnel », garant des droits fondamentaux (**II**).

I - La Charte des droits fondamentaux de l'Union européenne, norme de référence

Tout au long de sa motivation, la Cour de justice fait référence de façon itérative à la Charte, qui lui fournit à la fois le mètre étalon à l'aune duquel il convient de mesurer la légalité (« constitutionnalité ») de la directive (**A**), et la méthode lui permettant de procéder à ce contrôle (**B**).

A - La Charte, mètre étalon du contrôle

Les questions posées à la Cour de justice par la voie préjudicielle la conduisent à examiner directement la validité de la directive au regard de la Charte. Cela implique, d'une part, de vérifier la pertinence des articles de la Charte invoqués par les juridictions de renvoi (**1**) puis, d'autre part, de procéder à la qualification de l'ingérence dans les droits fondamentaux ainsi identifiés (**2**).

1 - Les références aux articles 7 et 8 de la Charte

La Cour se livre dans un premier temps à une lecture actualisée et synthétique de la directive (17), en constatant que celle-ci a pour « objectif principal » d'harmoniser les dispositions des États membres relatives à la conservation, par les fournisseurs de services de communications électroniques, de certaines données recueillies par ces fournisseurs, en vue de garantir leur disponibilité à des fins de lutte contre le terrorisme ou la criminalité grave, « dans le respect des droits consacrés aux articles 7 et 8 de la Charte » (18). La directive fait certes référence dans ses considérants à la Charte, mais cette dernière n'avait pas encore acquis le statut constitutionnel que lui a conféré le traité de Lisbonne. D'ailleurs, elle se limite dans son article 4 à poser l'exigence du respect des dispositions « du droit de l'Union européenne ou du droit international applicable en la matière, en particulier la Conv. EDH telle qu'interprétée par la Cour européenne des droits de l'homme ».

La « constitutionnalisation » de la Charte permet donc à la Cour désormais de faire l'économie du détour par la Conv. EDH, qui inspire et justifie habituellement son raisonnement, puisqu'elle peut fonder directement son argumentation sur cette source propre à l'Union. La démarche, pour n'être pas nouvelle (19), est particulièrement claire dans l'arrêt étudié. Ici, la double référence aux articles 7 et 8 de la Charte s'impose au regard de l'objet de la directive.

Les données recueillies et stockées par les fournisseurs de services de communications électroniques ne sont certes que des « métadonnées », c'est-à-dire ne concernent pas le contenu des communications (20), mais sont cependant suffisamment nombreuses et précises pour permettre, souligne la Cour « de tirer des conclusions très précises concernant la vie privée des personnes [...] telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci » (21). La Cour conclut ainsi sans difficulté que la conservation des données organisée par la directive « concerne de manière directe et spécifique la vie privée » (22) et tombe ainsi dans le champ d'application de l'article 7 de la Charte, consacré au droit au respect de la vie privée et familiale. Il va sans dire que l'article 8 de la Charte est également concerné, qui proclame le droit à la protection des données à caractère personnel. Les questions qui se posent sont donc celles de savoir si la conservation des données visées ne porte pas atteinte au droit au respect de la vie privée, d'une part, et si, d'autre part, les exigences relatives à la protection des données sont bien remplies.

Que la Cour de justice se fonde sur la seule Charte pour étayer son raisonnement semble justifié à plus d'un titre. Une Charte hissée au rang du droit primaire par le traité de Lisbonne fait en effet désormais partie des « normes de référence » pour le juge dans son office « constitutionnel ». La Charte présente ensuite l'avantage de consacrer un droit spécifique à la protection des données à caractère personnel, alors que, en revanche, il n'est que dérivé de l'article 8 Conv. EDH (relatif au droit au respect de la vie privée) par le juge de Strasbourg. Cette source à la fois spécifique et autonome simplifie et clarifie donc l'approche pour le juge de l'Union.

La norme de référence étant identifiée, la CJUE ne rencontre aucune difficulté dans un second temps pour procéder à la qualification de l'ingérence dans les droits fondamentaux garantis.

2 - La qualification de l'ingérence

S'agissant du droit à la protection des données, voir une ingérence dans la directive ne présente aucune difficulté, puisqu'il s'agit par définition de traitement de données à caractère personnel. L'avocat général dans ses conclusions (23) établit toutefois une distinction selon les données personnelles considérées, pour établir un lien - qui, selon lui, ne serait pas systématique - entre violation du droit au respect de la vie privée et violation du droit à la protection des données. Les articles 7 et 8 de la Charte sont certes étroitement liés, la Cour elle-même l'a déjà souligné (24), mais selon P. Cruz Villalon, tout dépend de la nature des données concernées. Il distingue en effet les données selon leur caractère plus ou moins « personnel » (25). Cette distinction pourrait être celle entre « informations nominatives » (P. Cruz Villalon parle de « données qui sont personnelles en tant que telles », dotées « d'une certaine neutralité ») et « données à caractère personnel » (26) (les données qui sont, selon P. Cruz Villalon, « plus que personnelles »). Les premières sont relatives « au nom et à ses accessoires » (27), les secondes sont « plus ouvertes à une multiplicité d'informations » (28), telles celles susceptibles de « cerner [l']individualité psychologique [de la personne] telle qu'elle se manifeste à travers ses comportements » (29), celles qui, « qualitativement, se rapportent essentiellement à la vie privée, au secret de la vie privée, en ce compris l'intimité », comme le note l'avocat général.

Si les deux catégories, subtilement distinguées, relèvent incontestablement du champ d'application de l'article 8 de la Charte, seule la seconde, en revanche, selon l'avocat général, permettrait de qualifier une ingérence dans le droit au respect de la vie privée garanti par l'article 7. Dans la mesure, en effet, où ces données se rapportent essentiellement « au secret de la vie privée » (30), ce n'est pas tant la question de la protection de ces données qui serait ici en question, mais plutôt le fait même que ces éléments de la vie privée d'une personne « aient pu se cristalliser sous la forme de données, susceptibles [...] d'être soumises à des traitements informatiques » (31). Le problème se présenterait donc prioritairement sous la forme d'une atteinte à l'article 7 et secondairement sous celle d'une atteinte à l'article 8. Dans la mesure où les données collectées peuvent « permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée » (32), l'avocat général identifie dans la directive « une ingérence particulièrement caractérisée dans le droit au respect de la vie privée » (33). La Cour juge plus simplement que l'obligation imposée aux fournisseurs de communications électroniques de conserver les données évoquées (métadonnées de communication) « constitue en soi une ingérence au sens de l'article 7 de la Charte » (34), en quelque sorte aggravée par l'accès à ces données ouvert aux autorités nationales compétentes. La Cour renforce son raisonnement en se référant à la jurisprudence correspondante de la Cour européenne des droits de l'homme (35), tout en conservant toutefois sa norme de référence spécifique, la Charte des droits fondamentaux de l'Union européenne en son article 7.

L'arrêt rendu par la Cour paraît majeur à plusieurs égards, notamment ici s'agissant de la qualification de l'ingérence, jugée « d'une vaste ampleur » et « comme particulièrement grave » (36). Le constat est sévère mais évident.

Ce qui ne peut manquer de frapper le lecteur en tout état de cause est la référence constante que fait la CJUE à la Charte, qui lui sert d'abord de « mètre étalon », et lui fournit ensuite la « boîte à outils » nécessaire pour passer la directive au crible de son analyse et de son contrôle.

B - La Charte, « boîte à outils » pour le contrôle

Jusqu'à la constitutionnalisation de la Charte des droits fondamentaux de l'Union, la Cour de justice se référait abondamment à la jurisprudence de son homologue strasbourgeoise. Elle semble s'en affranchir aujourd'hui (**1**), pour passer au seul crible de la Charte la question de la conformité aux droits fondamentaux (**2**).

1 - L'affranchissement vis-à-vis de la jurisprudence de la CEDH

Dans le cadre d'une Union européenne qui ne s'était pas encore dotée de son propre texte de référence en matière de droits fondamentaux, la CJUE s'appuyait, on le sait, sur la Conv. EDH aussi bien que sur les Principes généraux du droit communautaire qu'elle avait elle-même élaborés. Mais sans doute la promotion des droits de l'homme au rang de principes constitutionnels, déjà amorcée par le traité d'Amsterdam (37), a concouru au passage déterminant « d'une conception fonctionnelle à une conception constitutionnelle des droits fondamentaux » (38), entraînant « une mutation de l'ordre juridique communautaire ouvrant la perspective de la formation d'un droit communautaire des droits fondamentaux » (39). L'arrêt étudié est la parfaite illustration de cette mutation et fait apparaître par là même les conséquences d'une Charte « constitutionnelle » des droits fondamentaux de l'Union. Ces conséquences sont immenses quant à leur portée (nous y reviendrons), mais elles le sont aussi quant à la « méthodologie » suivie désormais par le juge de l'Union.

Dans sa jurisprudence antérieure au traité de Lisbonne, la Cour étayait donc principalement son raisonnement relatif à la protection des données à caractère personnel sur la jurisprudence de la CEDH, qui a fait une large place à ce nouveau droit par le biais de l'article 8 Conv. EDH consacré au droit au respect de la vie privée et familiale. Par exemple, dans l'arrêt *Osterreichischer Rundfunk* (40), la CJUE se réfère *expressis verbis* à l'article 8 Conv. EDH, et notamment à son paragraphe 2 subordonnant la régularité de l'ingérence dans le droit protégé au respect d'un certain nombre de garanties (41). Elle vérifie ainsi si la réglementation communautaire en question est justifiée au regard des conditions posées par l'article 8 Conv. EDH (42).

Déjà, dans l'arrêt *Volker und Markus Schecke & Eifert*, en date du 9 novembre 2010 (43), la Cour examine en revanche le litige sous l'angle de la Charte (tant au fond que sur la méthode), mais elle ne fait pas pour autant l'économie de toute référence à la Conv. EDH. Elle renvoie en effet, d'une part, aux définitions apportées par la jurisprudence de la CEDH en la matière et, d'autre part, aux limitations résultant de l'article 8, paragraphe 2, Conv. EDH.

Aujourd'hui, le cordon ombilical semble nettement coupé grâce à l'arrêt *Digital Rights Ireland*, qui voit tout le raisonnement de la Cour se baser sur la grille d'analyse fournie par la Charte et par elle seule.

2 - Une grille d'analyse se référant à la Charte

Afin d'évaluer la justification de l'ingérence, causée par la directive dans les droits garantis par les articles 7 et 8 de la Charte, la Cour adopte comme grille d'analyse les termes de l'article 52, paragraphe 1, de la Charte (44), qui détermine la portée des droits garantis en posant leurs limites. Il est aisé de constater que si l'idée est la même que dans l'article 8, paragraphe 2, Conv. EDH, la formulation n'est cependant pas identique (45).

Le juge s'intéresse donc tour à tour aux questions de savoir si la limitation de l'exercice du droit garanti est « prévue par la loi », si elle respecte son contenu essentiel, si elle respecte le principe de proportionnalité, si la limitation est nécessaire et si elle répond à des objectifs d'intérêt général reconnus par l'Union ou à un besoin de protection des droits et libertés d'autrui.

Ces différents points, d'inégale importance, sont traités avec plus ou moins d'ampleur par le juge. Ainsi, par exemple, la notion d'atteinte au contenu essentiel du droit fondamental au respect de la vie privée fait partie des éléments mineurs ici, le juge notant sans difficulté que, dans la mesure où la directive ne permet pas de prendre connaissance du contenu des communications électroniques, elle n'est pas de nature à porter atteinte au contenu du droit (46). Quant à la question de la nécessité des mesures de limitations apportées aux droits garantis, elle va être absorbée dans l'examen général de la proportionnalité, qui constitue un temps fort de l'arrêt. L'autre temps fort est celui consacré à la justification de l'ingérence par un objectif d'intérêt général.

À noter que le critère de la « prévisibilité » par la loi de la mesure restrictive de liberté, juste évoqué par le juge, est considérablement développé par l'avocat général dans ses conclusions. Celui-ci, se référant au demeurant à l'approche habituelle de la Conv. EDH relative à la « qualité de la loi », s'interroge sur le point de savoir si les limitations à l'exercice des droits fondamentaux que la directive comporte sont assorties de garanties suffisamment détaillées. Il semble au contraire que la directive s'en remette de façon générale aux États membres, ce que l'avocat général déplore, enjoignant par là même au législateur de l'Union à « jouer un rôle directeur » (47) dans la définition des garanties qui doivent encadrer la limitation des droits fondamentaux, ainsi qu'à « encadrer de façon principielle la très large délégation accordée aux États membres » (48) en la matière.

Mais si le juge de Luxembourg renvoie désormais uniquement à la Charte, en tant que norme et outil de référence pour son contrôle, il n'en manque pas pour autant de rendre un discret mais explicite hommage à son homologue de Strasbourg. En effet, il définit d'abord (en citant sa propre jurisprudence) le principe de proportionnalité, comme exigeant que les actes pris par l'Union afin de réaliser les objectifs légitimes prévus par la réglementation considérée, « ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs » (49). S'agissant ensuite du contrôle juridictionnel de la proportionnalité, il souligne clairement que « l'étendue du pouvoir d'appréciation » (50) du législateur de l'Union peut être limitée, en fonction de la nature du droit garanti, ainsi que de la nature, la gravité et la finalité de l'ingérence. Et il renvoie ici par analogie à l'arrêt de la CEDH, *S. et Marper c/ Royaume-Uni*, du 4 décembre 2008 (51), arrêt fondateur en matière de protection des données à caractère personnel (en particulier dans l'Espace de liberté, de sécurité et de justice), où le juge se livre à un remarquable contrôle de la proportionnalité, mettant en balance l'intérêt des individus à la protection de leur vie privée et l'intérêt général lié à la prévention des infractions pénales (52). Dans son analyse de « l'étendue du pouvoir d'appréciation » du législateur (formule qui renvoie naturellement au concept de « marge d'appréciation » employé à Strasbourg), la Cour de justice va procéder à un contrôle strict, eu égard à « l'ampleur » et à « la gravité » de l'ingérence constatée (53). Hommage n'est cependant pas servilité, et la Cour va ainsi développer sa propre analyse, en s'appuyant sur la base constitutionnelle désormais incontournable et qui lui est propre, la Charte des droits fondamentaux de l'UE.

Le juge de l'Union européenne va de la sorte se révéler en tant que véritable juge « constitutionnel », garant des droits fondamentaux de l'Union.

II - La Cour de justice, juge « constitutionnel » garant des droits fondamentaux

La CJUE, forte du nouvel appui constitutionnel que lui donne une Charte intégrée dans le droit primaire, se livre à un magistral examen de la directive contestée, qui lui permet de s'affirmer pleinement comme garante des droits fondamentaux. Elle opère à cet effet une surprenante lecture matérielle de la directive dans le cadre de la vérification de la justification de l'ingérence (**A**), puis procède à un contrôle strict de la proportionnalité, conduisant à l'annulation pure et simple de la directive (**B**).

A - La justification de l'ingérence : une surprenante lecture matérielle de la directive

Justifier l'ingérence produite par la directive dans les droits fondamentaux évoqués implique de démontrer sa nécessité, eu égard à l'objectif d'intérêt général que la directive est censée poursuivre. Cela revient à poser la question de la fonctionnalité de la directive, question éminemment délicate, puisque la Cour de justice, interrogée sur la base juridique de la même directive, y avait déjà donné une réponse. La lecture proposée aujourd'hui par l'avocat général Cruz Villalon

s'en éloigne substantiellement, par l'argument de la « dualité fonctionnelle » de la directive (**1**), qui va lui permettre en réalité de mettre l'accent sur le contenu de la directive, qui paraît désormais - et paradoxalement - comme « l'objectif prépondérant » poursuivi par celle-ci (**2**).

1 - La dualité fonctionnelle de la directive

Le terrain n'était pas vierge pour procéder à l'analyse de la directive, puisque la Cour de justice s'était déjà prononcée en 2009 sur la question de sa base juridique (54), à une époque où la construction de l'Union en piliers rendait parfois difficile l'aiguillage entre le pilier communautaire ou le troisième pilier (55). Certes, la Cour avait alors admis, dans un premier temps, que c'est dans le contexte de la lutte contre le terrorisme qu'avait été décidé d'imposer aux fournisseurs de services de conserver les données relatives aux communications électroniques. Mais elle avait souligné, dans un second temps, que les obligations de conservation desdites données entraînaient « des implications économiques substantielles pour les fournisseurs de services » (56). C'est donc l'objectif de protection du fonctionnement du marché intérieur qui aurait animé le législateur, en procédant ainsi à l'harmonisation nécessaire des législations nationales. Afin de justifier que l'acte trouve sa base légale dans le pilier communautaire, la Cour avait alors minimisé l'objectif de lutte contre le terrorisme que visait manifestement la directive (57), estimant que les dispositions de celle-ci n'impliquaient pas en soi une intervention des autorités répressives des États membres, et n'harmonisaient pas la question de l'accès aux données, ni celle de l'utilisation de ces données (questions relevant alors du troisième pilier). Son analyse lui a permis ainsi de conclure - la citation *in extenso* s'impose - que « le contenu matériel de la directive 2006/24 vise pour l'essentiel les activités des fournisseurs de services dans le secteur concerné du marché intérieur, à l'exclusion des activités étatiques relevant du titre VI du traité UE » (58), ainsi la directive « concerne de façon prépondérante le fonctionnement du marché intérieur » (59).

Dès lors, l'insistance avec laquelle l'avocat général souligne, dans les conclusions relatives à l'arrêt étudié, la « dualité fonctionnelle » de la directive laisse perplexe. C'est le souci de ne pas ouvertement remettre en cause l'arrêt de 2009 qui semble guider l'affirmation selon laquelle la « seconde fonction » de la directive, qualifiée « d'effet constitutif de l'obligation de conservation des données », doit être « particulièrement » prise en compte en l'espèce, mais sans pour autant « ignorer son effet spécifiquement harmonisateur des réglementations nationales » (60).

La dualité fonctionnelle de la directive pose problème, d'abord, quant au respect de la proportionnalité au sens de l'article 5, paragraphe 4, TUE (61), qui, avec le principe de subsidiarité, encadre et conditionne l'adoption de tous les actes de l'Union européenne. La proportionnalité doit-elle s'apprécier au regard des deux objectifs qu'elle poursuit (62), ou simplement au regard de celui considéré comme « prépondérant » ? Si cette deuxième option l'emporte, force est de constater que l'atteinte aux droits fondamentaux que la directive produit paraît disproportionnée par rapport à l'objectif poursuivi, qui est d'assurer un bon fonctionnement du marché intérieur. Ce qui permet à l'avocat général de constater très finement que les motifs qui sauvent la directive quant à sa base juridique, la perdent au regard de la proportionnalité (63). Mais il paraît difficile toutefois de justifier la proportionnalité de la directive en se fondant sur son objectif secondaire, dans la mesure précisément où elle a été validée quant à sa base juridique sur « l'objectif prépondérant » rattaché au marché intérieur. Pour éviter ainsi de mettre la Cour en porte à faux par rapport à son précédent arrêt, la vérification de la proportionnalité de l'article 5, paragraphe 4, TUE est purement et simplement écartée au profit de l'examen de la proportionnalité de l'article 52, paragraphe 1, déjà évoqué. Le juge, dans son arrêt, occulte donc totalement cette épineuse question.

2 - L'objectif matériel de la directive, « principal » à défaut d'être « prépondérant »

Répondre à la question de savoir si la directive poursuit un objectif d'intérêt général oblige le juge à identifier l'objectif principal (« prépondérant » ?) de celle-ci. Allant clairement au-delà des circonlocutions parfois embarrassées de l'avocat général (64), le juge n'hésite pas à constater que l'objectif « matériel » de la directive est bien « de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique » (65). Il s'appuie pour ce faire, d'abord, sur sa propre jurisprudence, qui a reconnu comme objectif d'intérêt général de l'Union la lutte contre le terrorisme international (66). Et il s'appuie ensuite sur l'article 6 de la Charte, qui énonce le droit de toute personne non seulement à la liberté mais également à la sûreté. Ce dernier argument confirme au demeurant l'approche purement autonome du juge, fondée sur la source juridique spécifique à l'Union désormais constitutionnalisée.

Sans prononcer explicitement les mots « objectif prépondérant », le juge estime que la conservation des données afin de permettre aux autorités nationales d'y accéder, moyen jugé comme « utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée » (67), « répond effectivement à un objectif d'intérêt général » (68).

Cette lecture matérielle de la directive permet ainsi à la Cour de prendre habilement le contrepied de ses affirmations antérieures sans véritablement se désavouer ou se contredire.

Il ne lui restait plus dès lors qu'à effectuer le contrôle de proportionnalité de cette directive, qui, tel Janus, présente deux faces mises tour à tour en lumière...

B - Un contrôle strict de la proportionnalité : une annulation intégrale de la directive

Le principe de proportionnalité exige, on l'a dit, que les actes pris par l'Union afin de réaliser les objectifs légitimes prévus par la réglementation considérée, « ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs » (69), sachant que « l'étendue du pouvoir d'appréciation » (70) du législateur de l'Union peut être limitée, en fonction de la nature du droit garanti, ainsi que de la nature, la gravité et la finalité de l'ingérence.

L'analyse de la Cour porte ici sur plusieurs points pouvant être décomposés sous la forme d'une question d'ordre général relative à l'objectif d'intérêt général poursuivi (déjà évoqué) permettant d'apprécier la nécessité de la législation (**1**), qui commande ensuite une série de questions plus spécifiques, liées à la problématique de la protection des données (**2**).

1 - La nécessité de l'ingérence au regard de l'objectif d'intérêt général poursuivi : un contrôle strict

L'objectif « d'arrière-plan » (71) de la directive, qui concentre en fait l'attention du juge en tant qu'objectif « matériel » (72) de celle-ci, est la lutte contre le terrorisme et la criminalité grave ou, en des termes plus généraux, un objectif de sécurité publique. La Cour convient d'abord sans difficulté que la conservation des métadonnées de communication dont il est question est tout à fait « apte à réaliser l'objectif poursuivi » (73). Il ne peut suffire à lui seul cependant à justifier la nécessité d'une telle ingérence causée dans les droits garantis par les articles 7 et 8 de la Charte, la Cour l'affirme clairement (74).

Empruntant son raisonnement à la CEDH mais sa référence à la Charte des droits fondamentaux de l'Union européenne, elle martèle que, eu égard à « l'importance particulière pour le respect du droit au respect de la vie privée » (75), que représente la protection des données à caractère personnel, la législation de l'Union doit non seulement prévoir des

règles claires et précises, mais également des « garanties suffisantes [...] contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données ». La nécessité de règles claires et précises est posée aussi par la Cour de Strasbourg afin de vérifier la « prévisibilité » de la loi (76), exigence commune au demeurant aux articles 8, paragraphe 2, Conv. EDH et 52, paragraphe 1, de la Charte (77). Cependant, même si la directive s'en remet, par nature, aux États membres, pour définir les garanties qui doivent entourer l'accès aux données en question, l'avocat général ne manque pas de souligner « le rôle directeur » que doit jouer ici le législateur de l'Union dans la définition de ces garanties (78). C'est une véritable injonction qu'il lui adresse en la matière (79), et le juge lui emboîte le pas en estimant que la directive « ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire » (80).

Il reste à voir les arguments - et la liste est longue - qui ont conduit la Cour à un jugement aussi sévère, mais auquel on ne peut que souscrire.

2 - Des garanties insuffisantes pour limiter l'ingérence au strict nécessaire

La stricte nécessité de l'ingérence semble difficile à justifier, d'abord, pour un mécanisme de collecte et de conservation de données qui « vise tous les moyens de communication électronique » et, surtout, concerne « la quasi-totalité de la population européenne » (81), créant ainsi « un sentiment diffus de surveillance » (82).

La Cour condamne ensuite l'application de la directive de façon globale, indifférenciée, c'est-à-dire « même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves ». Cette démarche est l'exemple type d'une approche « proactive » (83), qui vise à voir un possible suspect dans toute personne innocente (84), et qui a été vigoureusement condamnée dans son principe aussi bien par le Contrôleur européen de la protection des données (85) que par le « Groupe de l'article 29 » (86). Aujourd'hui, c'est la Cour de justice qui épingle cette méthode, et sa condamnation est majeure et risque de s'avérer lourde de conséquences. En effet, nombre de dispositifs de recueil et de traitement de données organisés à des fins de lutte contre le terrorisme ou la grande criminalité mettent en oeuvre cette logique proactive, telle par exemple la future directive « PNR » européenne (87). Le législateur sera donc tenu de prendre en compte la sérieuse mise en garde formulée ici par la Cour, qui pose avec clarté les limites à ne pas franchir.

Un autre motif de censure de la directive 2006/24/CE apparaît ensuite dans ses dispositions encadrant insuffisamment les conditions matérielles et procédurales d'accès des autorités nationales compétentes aux données concernées. C'est en particulier la violation du principe, cardinal en la matière, de limitation des finalités qui est visée ici. Ce principe implique qu'un traitement de données à caractère personnel ne peut avoir lieu que dans le cadre d'une finalité strictement délimitée, sans utilisation ultérieure possible pour une finalité distincte. Il y est manifestement porté atteinte par la directive qui ne contient « aucun critère objectif permettant de limiter [...] l'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi » (88).

La question de la durée de conservation des données ne manquera pas de susciter l'intérêt de diverses cours constitutionnelles européennes qui déjà s'en étaient émues, en particulier la Cour constitutionnelle allemande (89). Cette durée, qui se situe entre six mois au minimum et vingt-quatre mois au maximum, là encore sans fixation de critères objectifs assurant qu'elle soit limitée au strict nécessaire (90), n'est pas jugée « nécessaire » par l'avocat général, qui se livre en ses conclusions à une belle -et quasi philosophique - réflexion sur le temps (91)... La Cour le confirme, de façon plus brève mais sans appel.

Le dernier motif d'inquiétude (et pas le moindre) est le risque que les données en cause soient conservées en dehors du territoire de l'Union (92). Ceci signifie que ne serait pas garanti le contrôle par une autorité indépendante, « explicitement exigé par l'article 8 paragraphe 3 de la Charte » (93) souligne la Cour, qui au demeurant a déjà insisté dans sa jurisprudence sur l'importance de ce paramètre en tant qu'élément essentiel du droit à la protection des données (94).

La conclusion, pour la Cour, s'impose d'elle-même : la directive n'a pu passer avec succès le strict contrôle de proportionnalité, elle est donc déclarée invalide. Qui plus est, c'est dans son intégralité et *ab initio* qu'elle est jugée invalide, cas rarissime qui va obliger « les institutions de l'Union à remédier au plus vite aux effets de leur inconséquence » (95).

S'il est un enseignement que l'on peut tirer de cet arrêt, c'est sans nul doute celui des conséquences qui s'attachent désormais à la place occupée par la Charte des droits fondamentaux de l'Union, à savoir la première. À l'image d'un palimpseste, cet arrêt est toutefois aussi important par son discours implicite que par sa décision, historique il faut le répéter. Si l'Europe des citoyens paraît en panne, celle des juges est entrée depuis quelque temps dans une phase de maturité, pour le plus grand bienfait des droits fondamentaux. Comment ne pas voir en effet plus qu'une coïncidence entre l'arrêt rendu et les gestes de conciliation récents des cours constitutionnelles européennes, tels le Conseil constitutionnel français ou la Cour constitutionnelle allemande, acceptant désormais de saisir la Cour de justice d'un renvoi préjudiciel (96) ? La Cour constitutionnelle allemande qui, avec d'autres, s'était inquiétée du contenu de la directive 2006/24/CE (97), ne peut que se réjouir de voir son raisonnement ainsi validé par la Cour de justice de l'Union, et son avertissement entendu (98). La Charte des droits fondamentaux de l'Union, grâce à son inscription dans le droit primaire, devient donc la solide pierre angulaire sur laquelle le juge de l'Union peut dorénavant s'appuyer, contribuant de la sorte à sa mutation en véritable juge constitutionnel, gardien des droits fondamentaux. La garantie de la protection des données à caractère personnel - souvent mise à mal dans un souci de sécurité publique, il ne faut pas l'oublier - semble ainsi désormais pleinement assurée. Nul doute qu'à la lumière de cet arrêt, bien des textes en ce domaine actuellement examinés par le législateur (99) vont lui donner matière à réflexion.

Mots clés :
DROIT ET LIBERTE FONDAMENTAUX * Charte européenne des droits fondamentaux * Application * Protection des données à caractère personnel * Lutte anti-terrorisme * Cour de justice de l'Union européenne * Droit constitutionnel
DROIT COMMUNAUTAIRE ET DROIT DE L'UNION EUROPEENNE * Intérêt général * Principe de proportionnalité * Dualisme

(1) V. M.-C. de Montecler, AJDA 2014. 773 .

(2) Arrêt de la Cour (gr. ch.) du 8 avr. 2014, aff. jtes C-293/12 et C-594/12, *Digital Rights Ireland Ltd & Kärntner Landesregierung, Seitlinger, Tschohl et a*.

(3) Citons pour exemple l'important arrêt de la Cour constitutionnelle allemande du 2 mars 2010, BVerfGE 118,79 (sur la question de la durée de rétention des données, v. *infra* II, B, 2°, et note 83). V. aussi Cour constitutionnelle roumaine, décis. du 8 oct. 2009, n° 1.258 (pour une traduction en anglais, v. : http://www.ccr.ro/files/products/D1258_091.pdf) ; v. à ce propos ci-dessous note 84. V. encore : Cour constitutionnelle tchèque, arrêt du 22 mars 2011, Pl. US 24/10, qui s'est interrogée notamment sur la question de la proportionnalité ; pour une traduction en anglais : www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D[egal]40&cHash[egal]bbaa1c5b1a7d6704af6370fdfce5d34c ; ou la Cour administrative suprême bulgare, décis. du 11 déc. 2008, n° 13627 ; ou encore la Cour suprême chypriote, décis. du 1er févr. 2011, n° 183(I)/2007.

(4) V. son arrêt du 10 févr. 2009, aff. C-301/06, *Irlande c/ Parlement européen et Conseil*.

(5) Elle défend les droits fondamentaux « à l'ère numérique ». V. www.digitalrights.ie/about/.

(6) V. N. Vandystadt, Cour de justice : une directive antiterrorisme sur la sellette, Europolitics, n° 4846, mardi 8 avr. 2014, p. 8.

(7) Concl. av. gén. Cruz Villalon, 12 déc. 2013, aff. jtes C-293/12 et C-594/12.

(8) Ci-dessous, « la Charte ».

(9) Celui-ci, estimant que les États membres « ont, de façon générale [...] exercé leurs compétences avec modération pour ce qui est de la durée maximale de conservation des données » (§ 157 de ses concl.), proposait en effet de « tenir en suspens les effets du constat d'invalidité de la directive [...], le temps que le législateur de l'Union prenne les mesures nécessaires pour remédier à l'invalidité constatée, étant précisé que ces mesures doivent intervenir dans un délai raisonnable » (§ 158).

(10) V. H. Labayle, La Cour de justice et la protection des données : quand le juge européen des droits fondamentaux prend ses responsabilités, 9 avr. 2014, http://www.gdr-elsj.eu/2014/04/09/cooperation-judiciaire-penale/la-cour-de-justice-et-la-protection-des-donnees-quand-le-juge-europeen-des-droits-fondamentaux-prend-ses-responsabilites/.

(11) E. Snowden, rappelons-le, était informaticien et travaillait pour différents sous-traitants de la *National Security Agency* (NSA), l'agence de renseignements américaine.

(12) Et à la mémoire courte. En effet, les États-Unis alliés avec le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande (les *Five Eyes*) ont mis en place dans les années 1970 un programme de recueil d'informations à l'échelle planétaire : le réseau Échelon, qui avait pour but d'intercepter puis d'analyser les communications téléphoniques et électroniques, aussi bien privées que publiques.

(13) Art. 52, § 1 : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

(14) À l'image de la Constitution, du bloc de constitutionnalité, pour une juridiction constitutionnelle.

(15) V. l'art. 2 du traité de Lisbonne : « 1. L'Union a pour but de promouvoir la paix, ses valeurs et le bien-être de ses peuples ».

(16) Par l'art. 6 du traité qui inscrit la Charte des droits fondamentaux dans le droit primaire.

(17) Dans la mesure où elle l'avait déjà examinée dans le cadre d'un recours en annulation, et avait validé sa base juridique ancrée dans le pilier « marché intérieur ». Elle avait estimé alors que son « objectif prépondérant » (nous y reviendrons) concernait le fonctionnement du marché intérieur (v. § 85 de l'arrêt du 10 févr. 2009).

(18) V. § 24 de l'arrêt.

(19) V. par ex. l'arrêt *Commission c/ The Bavarian Lager Co. Ltd*, 29 juin 2010, aff. C-28/08 P, ou encore l'arrêt CJUE 24 nov. 2011, aff. C-70/10, *Scarlet Extended*, D. 2011. 2925, obs. C. Manara ; *ibid*. 2012. 2343, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *ibid*. 2836, obs. P. Sirinelli ; RSC 2012. 163, obs. J. Francillon ; RTD eur. 2012. 404, obs. F. Benoît-Rohmer ; *ibid*. 957, obs. E. Treppoz .

(20) Il s'agit de toutes les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication ainsi que le matériel de communication des utilisateurs. Parmi ces données figurent, notamment, le nom et l'adresse de l'abonné inscrit, le numéro de téléphone de l'appelant et le numéro appelé, l'adresse IP pour les services internet, le temps de communication, le lieu à partir duquel elle a eu lieu, la fréquence des communications.

(21) V. § 27.

(22) V. § 29.

(23) Concl. av. gén. Cruz Villalon, préc.

(24) V. CJUE 9 nov. 2010, aff. jtes C-92/09 et C-93/09, *Volker und Markus Schecke & Eifert*, RTD eur. 2011. 375, chron. A. Potteau, § 47 : « À cet égard, il importe de relever que l'article 8, paragraphe 1, de la Charte énonce que "[t]oute personne a droit à la protection des données à caractère personnel la concernant". Ce droit fondamental est étroitement lié au droit au respect de la vie privée consacré à l'article 7 de cette même Charte ».

(25) Il parle de « données qui sont personnelles en tant que telles » et de « données qui sont en quelque sorte plus que personnelles » : v. les § 64-65 de ses concl.

(26) V. J. Eynard, *Les données personnelles. Quelle définition pour un régime de protection efficace ?*, Éd. Michalon, Paris, 2013, p. 53.

(27) *Ibid.*

(28) *Ibid.*

(29) *Ibid.* p. 68.

(30) V. P. Cruz Villalon, dans ses concl. préc., § 65.

(31) *Ibid.*

(32) V. § 74 de l'arrêt.

(33) V. § 80.

(34) V. § 34.

(35) Par ex. CEDH 26 mars 1987, série A n° 116, *Leander c/ Suède*, ou encore CEDH 4 mai 2000, req. n° 28341/95, *Rotaru c/ Roumanie*, AJDA 2000. 1006, chron. J.-F. Flauss ; D. 2001. 1988, obs. A. Lepage.

(36) V. § 37.

(37) En ce sens qu'au titre de l'art. 6, § 1, du traité d'Amsterdam, « l'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'État de droit, principes qui sont communs aux États membres ».

(38) V. F. Sudre et R. Tinière, *Droit communautaire des droits fondamentaux*, éd. Nemesis, Bruxelles, 2012, p. 17.

(39) *Ibid.*

(40) CJCE 20 mai 2003, aff. jtes C-465/00, C-138/01 et C-139/01, AJDA 2003. 2146, chron. J.-M. Belorgey, S. Gervasoni et C. Lambert.

(41) L'art. , § 2, Conv. EDH reconnaît la possibilité d'une ingérence à condition qu'elle soit « prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

(42) V. par ex. § 71-72 de l'arrêt préc.

(43) Soit quasiment un an après l'entrée en vigueur du traité de Lisbonne (1er déc. 2009). V. note 22.

(44) Celui-ci dispose que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ». Pour un commentaire détaillé, v. par ex. : J. Meyer, *Kommentar zur Charta der Grundrechte der Europäischen Union*, Nomos Verlagsgesellschaft, Baden-Baden, 2003, p. 577 s.

(45) V. ci-dessus, note 41.

(46) V. § 39 de l'arrêt.

(47) V. § 117 de l'arrêt.

(48) V. § 118 de l'arrêt.

(49) V. § 46 de l'arrêt.

(50) V. § 47 de l'arrêt.

(51) CEDH 4 déc. 2008, req. n^{os} 30562/04 et 30566/04, AJDA 2009. 872, chron. J.-F. Flauss ; D. 2010. 604, obs. J.-C. Galloux et H. Gaumont-Prat ; AJ pénal 2009. 81, obs. G. Roussel ; RFDA 2009. 741, étude S. Peyrou-Pistouley ; RSC 2009. 182, obs. J.-P. Marguénaud.

(52) V. par ex. notre commentaire, L'affaire *Marper c/ Royaume-Uni*, un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité et justice de l'Union européenne, RFDA 2009. 741.

(53) V. ci-dessus A.

(54) V. CJCE, gr. ch., 10 févr. 2009, aff. C-301/06, *Irlande, soutenue par Slovaquie, c/ Parlement européen et Conseil, soutenus par Espagne, Pays-Bas, Commission, Contrôleur européen de la protection des données*.

(55) On pourrait rappeler à cet égard l'important contentieux ayant mené à l'annulation de la décision relative à la conclusion de l'accord « PNR », CJCE 30 mai 2006, aff. C-317/04 et C-318/04, *UE c/ États-Unis*, D. 2006. 1560, obs. E. Pahlawan-Sentilhes ; AJ pénal 2006. 369, obs. C. Saas ; RSC 2006. 684, chron. L. Idot ; RTD eur. 2006. 535, note V. Michel. Dans ce cas, ce sont les finalités de sécurité publique de prévention et de répression du terrorisme qui ont prévalu, conduisant à l'annulation d'actes pris sur le fondement du pilier communautaire.

(56) V. § 68 de l'arrêt du 10 févr. 2009.

(57) L'*ultima ratio* de celle-ci étant de pouvoir mettre à disposition des autorités répressives les données de communication électroniques, moyen jugé comme « efficace pour détecter et réprimer les infractions pénales, y compris le terrorisme », § 67 de l'arrêt.

(58) V. § 84 de l'arrêt du 10 févr. 2009.

(59) V. § 85 de l'arrêt du 10 févr. 2009.

(60) V. § 47 de l'arrêt du 8 avr. 2014.

(61) Art. 5, § 4 : « En vertu du principe de proportionnalité, le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités ».

(62) À savoir l'harmonisation des législations nationales aux fins du bon fonctionnement du marché intérieur, d'une part, et la garantie de l'accès aux données par les autorités répressives aux fins de lutte contre le terrorisme et la grande criminalité, d'autre part.

(63) V. § 102 de l'arrêt.

(64) Celui-ci souligne par exemple que l'objectif « prépondérant n'est pas l'objectif « exclusif », et « qu'il existe bien un espace impliquant que dans le cadre de l'examen de la proportionnalité [...] soit pris en considération l'objectif ultime de répression des activités criminelles les plus graves qu'elle poursuit », § 103 des concl.

(65) V. § 41 de l'arrêt.

(66) Il se réfère ainsi par exemple à son célèbre arrêt du 3 sept. 2008, aff. C-402/05 P et C-415/05 P, *Kadi et Al Barakaat International Foundation c/ Conseil et Commission*.

(67) V. § 43 de l'arrêt.

(68) V. § 44 de l'arrêt.

(69) V. § 46 de l'arrêt.

(70) V. § 47 de l'arrêt.

(71) Selon les termes de l'av. gén., v. § 104 de ses concl.

(72) V. § 41 de l'arrêt.

(73) V. § 49 de l'arrêt.

(74) « Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte », § 51.

(75) V. § 53 de l'arrêt.

(76) V. par ex. : CEDH 1er juill. 2008, req. n° 58243/00, *Liberty et a. c/ Royaume-Uni*, § 60 ; CEDH 4 mai 2000, req. n° 28341/95, *Rotaru c/ Roumanie*, AJDA 2000. 1006, chron. J.-F. Flauss ; D. 2001. 1988, obs. A. Lepage, § 57-59.

(77) V. la lettre de l'art. 8, § 2, Conv. EDH ci-dessus, note 41, et celle de l'art. 52, § 1, de la Charte, note 44.

(78) V. § 117 des concl.

(79) V. § 120 *in fine* : « Il doit, sous peine de vider de leur sens les dispositions de l'article 51 paragraphe 1 de la Charte, pleinement assumer sa part de responsabilité en définissant à tout le moins les principes devant présider à la définition, l'établissement, à l'application et au contrôle du respect de ces garanties ».

(80) V. § 65 de l'arrêt.

(81) V. § 56.

(82) Comme le souligne l'avocat général (§ 72 de ses concl.), citant lui-même la Cour constitutionnelle allemande, qui s'était prononcée sur la question de la constitutionnalité de la directive (Décis. du 2 mars 2010, 1 BvR 256/08, 1 BvR 263/08 et 1 BvR 586/08),

www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

(83) Elle consiste à définir et analyser des critères d'évaluation mis en oeuvre afin d'évaluer le risque que peuvent représenter les personnes.

(84) C'est un argument majeur qui a été soulevé par exemple par la Cour constitutionnelle roumaine, qui a jugé trop large le champ d'application de la législation, estimant : « It would transform a priori all users of electronic communication services or public communications networks into people suspected of committing terrorism crimes or other serious crimes » (v. Murphy, *Romanian constitutional court decision n° 1258 of 8 october 2009*, 47 CML Rev.[2010], 933-941).

(85) V. son avis sur la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives présentée par la Commission le 6 nov. 2007, JOUE n° C 110, 1er mai 2008, p. 1, § 35.

(86) Groupe de l'art. 29, prévu par l'art. 29 de la Dir. 95/46/CE du Parlement européen et du Conseil du 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE n° L 281 du 23 nov. 1995, p. 31 s. V. ici Groupe de travail « Article 29 » sur la protection des données et Groupe de travail sur la police et la justice, Avis commun sur la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers(PNR) à des fins répressives présentée par la Commission le 6 nov. 2007, art. 29 réf. WP 145 / WPPJ réf. 01/072, concl. p. 14.

(87) V. la proposition de directive relative à l'utilisation des données des dossiers passagers *(Passenger Name Record, PNR)* pour la prévention et la détection des infractions terroristes et les formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, COM(2011)32 final, du 2 févr. 2011.

(88) V. § 62 de l'arrêt.

(89) V. sa décision mentionnée ci-dessus note 3.

(90) Et sans que soit opérée par exemple une quelconque distinction entre les catégories de données prévues (v. § 63 de l'arrêt).

(91) V. les § 145-152.

(92) « Dans des lieux indéterminés du cyberespace », selon les mots (presque poétiques !) de l'avocat général faisant

évidemment allusion au « cloud computing » ou « informatique en nuage » (§ 144 de ses concl.).

(93) V. § 68 de l'arrêt.

(94) V. l'arrêt CJUE 9 mars 2010, aff. C-518/07, *Commission c/ RFA*, AJDA 2010. 937, chron. M. Aubert, E. Broussy et F. Donnat ; RFDA 2011. 377, chron. L. Clément-Wilz, F. Martucci et C. Mayeur-Carpentier, ainsi que l'arrêt CJUE 16 oct. 2012, aff. C-614/10, *Commission c/ Autriche*, RTD eur. 2013. 671, obs. F. Benoît-Rohmer.

(95) V. H. Labayle, déjà cité, « La Cour de justice et la protection des données : quand le juge européen des droits fondamentaux prend ses responsabilités », 9 avr. 2014,

http://www.gdr-elsj.eu/2014/04/09/cooperation-judiciaire-penale/la-cour-de-justice-et-la-protection-des-donnees-quand-le-juge-europeen-des-droits-fondamentaux-prend-ses-responsabilites/.

(96) V. Cons. const. 14 juin 2013, n° 2013-314 QPC, D. 2013. 1805, note J.-C. Bonichot ; AJ pénal 2014. 44 ; RFDA 2013. 691, note H. Labayle et R. Mehdi ; RSC 2013. 903, obs. B. de Lamy ; RTD civ. 2013. 564, obs. P. Puig ; RTD eur. 2013. 531, note J. Roux ; Cour constitutionnelle de la RFA (*Bundesverfassungsgericht*), 14 janv. 2014 (v. communiqué de presse du 7 févr. 2014, Réf. n° 9/2014).

(97) V. Décision préc. du 2 mars 2010, BVerfGE 118,79. La Cour allemande avait estimé que la question de la durée maximale de rétention des données touchait aux droits fondamentaux garantis par la loi fondamentale allemande, et donc à « l'identité constitutionnelle » de la RFA.

(98) L'arrêt de la Cour de justice traduit donc manifestement son désir « to reassure national constitutional courts by emphasizing the EU's commitment to fundamental rights », Orla Lynskey, The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety, CML Rev. 51 (2014), 1789-1812 (p. 1801).

(99) Refonte de la Dir. 95/46/CE du 24 oct. 1995, texte de base en matière de protection des données, ainsi que de la décision-cadre 2008/977/JAI du 27 nov. 2008, relative à la protection des données dans l'ex-troisième pilier. Ont été présentées par la Commission le 25 janv. 2012 une proposition de règlement et une proposition de directive, appelés à remplacer ces textes, v. respectivement COM(2012)11 final et COM(2012)10 final. À signaler aussi l'adoption en cours d'un « PNR » européen, v. COM(2011)32 final du 2 févr. 2011.

Copyright 2015 - Dalloz – Tous droits réservés