«Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données»

Peter Hustinx[*]

1. Introduction

Le concept de «protection des données» est apparu il y a près de quarante ans afin d'offrir aux personnes une protection juridique contre l'utilisation inappropriée des technologies de l'information aux fins du traitement de données les concernant. Il n'a pas été conçu pour *empêcher* le traitement de ces informations ni pour *limiter* l'utilisation des technologies de l'information en soi, mais pour donner des garanties chaque fois que des technologies de l'information sont utilisées pour traiter des données concernant des personnes. Ce concept reposait sur la conviction, acquise très tôt, que l'utilisation intensive des technologies de l'information à cet effet pourrait produire des conséquences d'une portée considérable pour les droits et les intérêts des personnes.[1]

En d'autres termes, la protection des données était une question liée aux droits et aux intérêts des personnes, et non principalement aux données concernant ces personnes, contrairement à ce que la terminologie utilisée indique. En tout état de cause, ce concept a été inventé à une époque où l'utilisation omniprésente des technologies de l'information en était encore à ses débuts. Aujourd'hui, les choses ont bien changé et les conséquences potentielles d'une telle utilisation - par suite de l'avènement de l'internet et des appareils portables - nous entourent, à chaque minute de chaque jour, dans nos vies à la fois personnelle et professionnelle. Cette situation risque encore de s'amplifier à l'avenir. Il convient dès lors d'examiner l'état actuel du droit européen sur la protection des données dans le contexte d'un cours sur le droit de l'Union et les technologies.

Une autre raison qui explique l'importance du droit européen sur la protection des données est que son principal instrument à l'heure actuelle - la directive 95/46/CE, aussi appelée «directive sur la protection des données» - fait aujourd'hui l'objet d'une révision de grande

---

[*] Contrôleur européen de la protection des données (2004-2014). Le présent article est basé sur un cours dispensé à l'Académie de droit européen de l'Institut universitaire européen, 24e session sur le droit de l'Union européenne, du 1er au 12 juillet 2013. Il se fonde aussi sur des informations tirées de multiples articles et discours publiés par l'auteur ces dernières années, tels que Hustinx, P.J., «Gegevensbescherming in de informatiemaatschappij», dans Numan, E.J., *et al.* (ed.), *Massificatie in het privaatrecht* (2010), pages 77-91, et Hustinx, P., «Loi européenne relative à la protection des données - situation actuelle et perspectives d'avenir», discours prononcé lors de la conférence de haut niveau: «Dimensions éthiques de la protection des données et de la vie privée», Centre pour l'éthique, Université de Tartu / Inspection de la protection des données, Tallinn, Estonie, 9 janvier 2013, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_FR.pdf (dernière consultation le 31 mai 2014). L'auteur tient à remercier C. Docksey pour ses observations sur le projet d'article.

[1] Voir la section 2 ci-dessous.

ampleur visant à lui conférer davantage d'efficacité dans un monde où les technologies de l'information jouent un rôle éminent dans tous les domaines de la vie, à la fois publique et privée. Cette révision arrive au stade final du processus décisionnel politique: le Parlement européen et le Conseil se préparent aux négociations qui aboutiront à la mise en place du futur cadre juridique de l'Union européenne sur la protection des données, qui restera probablement en vigueur pendant quelques décennies. Pour cette raison, l'heure est venue de faire le point sur le droit de l'Union sur la protection des données et d'examiner de plus près certaines questions essentielles.[2]

Le contexte de la révision ne fait qu'accroître l'importance de cet exercice. Outre le caractère dynamique de notre environnement numérique et l'ambition de tirer parti de ces évolutions dans une stratégie numérique qui contribue à la croissance économique, nous avons également découvert récemment que cet environnement était plus vulnérable que la plupart le supposait. Les révélations sur la surveillance à grande échelle de nos comportements en ligne par l'Agence pour la sécurité nationale américaine et d'autres services de renseignement ont, à juste titre, provoqué une onde de choc à travers le monde. D'autre part, il est désormais évident que de nombreuses pratiques commerciales en ligne, dont certaines des plus populaires, reposent également sur une surveillance intensive du comportement des consommateurs. De même, l'offre grandissante de services «gratuits» en échange de la surveillance a ouvert la porte à un espionnage à grande échelle par d'autres acteurs. Ainsi, la révision du cadre juridique de l'Union européenne sur la protection des données se déroule dans un contexte où la nécessité d'une protection plus efficace et les difficultés que pose la concrétisation de cette protection dans la pratique se sont considérablement accrues. Bien que nous ne soyons pas en mesure de répondre à toutes les questions pertinentes, il serait toujours utile d'examiner certaines des solutions qui sont en cours d'élaboration pour relever ces défis.

Dans cet article, nous aborderons aussi les origines de la législation européenne sur la protection des données, ainsi que les différences entre la «vie privée» et la «protection des données» qui ont contribué à son évolution par la suite. Il est en effet nécessaire de mieux comprendre ces éléments pour appréhender les problèmes susceptibles de survenir eu égard aux cadres juridiques actuel et futur. Il existe également d'importantes connexions entre ces deux concepts. La vie privée et la protection des données - plus précisément, le droit au *respect* de la vie privée et le droit d'une personne à la *protection* de ses données à caractère personnel - sont toutes deux des expressions plutôt récentes d'une idée universelle qui revêt de fortes dimensions éthiques: la dignité, l'autonomie et la *valeur unique* de tout être humain. Cette idée associe également le droit de chaque personne à développer sa propre personnalité et à avoir son mot à dire sur des questions susceptibles d'avoir une incidence directe sur elle. Elle explique deux caractéristiques qui ressortent fréquemment à cet égard: la nécessité d'empêcher les *immixtions* injustifiées dans les questions d'ordre privé et la nécessité de

[2] Voir notamment les sections 5 à 7 ci-dessous.

garantir à chaque personne un *contrôle* approprié sur les questions susceptibles de les concerner.

Ces quarante dernières années, la vie privée et la protection des données, en tant que domaine spécifique du droit, se sont développées à l'échelon européen, notamment dans le cadre du Conseil de l'Europe dans un premier temps, puis essentiellement dans celui de l'Union européenne. Cependant, comme l'Union a poursuivi ses travaux sur la base de ceux du Conseil de l'Europe, nous nous pencherons sur les deux afin d'avoir une vue d'ensemble. Cette vue d'ensemble fera ressortir deux axes principaux: le premier a trait au développement de droits à la vie privée et à la protection des données *plus forts* et le deuxième à la nécessité de garantir une application *plus cohérente* de ces droits à travers l'Union européenne. Ces deux axes visent à promouvoir une protection concrète *plus efficace* et d'éviter une *diversité inutile* dans la manière dont cette protection est assurée dans les États membres. Ces deux axes présentent une évolution progressive à des stades différents, marquée aussi désormais par une influence croissante de la charte des droits fondamentaux, à la fois dans la jurisprudence de la Cour de justice et dans la révision de l'actuel cadre juridique. La mention séparée de la «vie privée» et de la «protection des données» dans la charte soulève des questions quant à la distinction entre les deux concepts.

Le présent article suivra largement un fil chronologique: les origines de la protection des données et le rôle du Conseil de l'Europe seront abordés à la section 2, puis viendront les grandes lignes de l'actuelle directive de l'Union à la section 3. Après un intermède à la section 4 sur différents aspects institutionnels, y compris la charte et l'incidence du traité de Lisbonne, nous nous pencherons (section 5) sur le contexte et les principaux axes de la proposition de règlement général sur la protection des données. À la section 6, nous mettrons en évidence certaines questions clés de l'actuel débat législatif et, à la section 7, nous aborderons d'autres questions susceptibles d'appeler une réflexion et une discussion plus approfondies. Enfin, nous formulerons quelques observations finales à la section 8.

2. Les origines de la protection des données

A. Vie privée

Ce n'est qu'après la Seconde Guerre mondiale que le concept de «droit à la vie privée» a vu le jour en droit international. Il est d'abord apparu sous une forme relativement atténuée à l'article 12 de la Déclaration universelle des droits de l'homme[3], qui prévoit que nul ne sera l'objet d'immixtions *arbitraires* dans sa vie privée, sa famille, son domicile ou sa correspondance.

[3] Assemblée générale de l'ONU, Paris, 1948.

Une protection plus concrète a ensuite été garantie par l'article 8 de la Convention européenne des droits de l'homme (CEDH)[4], qui prévoit que toute personne a droit au *respect* de sa vie privée et familiale, de son domicile et de sa correspondance, et qu'il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à certains intérêts importants et légitimes.

La mention du «domicile» et de la «correspondance» reposait sur des traditions constitutionnelles inhérentes à de nombreux pays du monde et héritées d'une longue évolution, de plusieurs siècles parfois, mais l'accent placé sur la vie privée constituait une nouveauté et une réaction manifeste à ce qui s'était passé au cours de la Seconde Guerre mondiale.

La portée et les conséquences de cette protection ont été expliquées dans une série d'arrêts de la Cour européenne des droits de l'homme.[5] Dans toutes ces affaires, la Cour examine - en bref - s'il y a une *ingérence* dans le droit au respect de la vie privée et, dans l'affirmative, si cette ingérence est justifiée par une base juridique *appropriée* - c'est-à-dire claire, accessible et prévisible - et si elle est *nécessaire* et proportionnée à l'intérêt légitime en jeu.

B. Protection des données

Au début des années 1970, le Conseil de l'Europe est arrivé à la conclusion que l'article 8 de la CEDH présentait un certain nombre de lacunes au vu des évolutions récentes, en particulier compte tenu de l'utilisation croissante des technologies de l'information: la portée incertaine de la notion de «vie privée», l'accent mis sur la protection contre les ingérences des «autorités publiques» et le manque d'approche plus proactive contre les éventuelles utilisations abusives d'informations à caractère personnel commis par des entreprises ou d'autres organisations concernées appartenant au secteur privé.[6]

Deux recommandations du Comité des ministres aux États membres ont suivi, le but étant d'adopter toutes les mesures nécessaires visant à donner effet à certains principes de la protection de la vie privée des personnes dans les secteurs privé et public.[7] Ces

[4] Conseil de l'Europe, Rome, 1950
[5] Voir la section 2, partie D, ci-dessous.
[6] Rapport explicatif sur la Convention 108 (voir note de bas de page 9 ci-dessous), paragraphe 4.
[7] Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, et résolution (74) 29 relative à la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public.

recommandations ont coïncidé avec les premières initiatives nationales dans des pays comme l'Allemagne et la Suède.[8]

Les expériences positives qu'ont constituées ces premières initiatives ont encouragé le Conseil de l'Europe à investir du temps dans la préparation d'un accord international appelé à devenir le premier instrument contraignant en la matière. Après quatre ans, la Convention pour la protection des données, également connue sous le nom de Convention 108[9], a été adoptée; à ce jour, 46 pays l'ont ratifiée, au nombre desquels figurent l'ensemble des États membres de l'Union européenne, la plupart des États membres du Conseil de l'Europe et un pays tiers.[10]

La Convention a pour but de garantir, sur le territoire de chaque partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»).[11] La notion de «données à caractère personnel» y est définie comme «toute information concernant une personne physique identifiée ou identifiable ("personne concernée")».[12]

Ainsi, «la protection des données» revêt une portée à la fois *plus large* que la «protection de la vie privée» en ce qu'elle concerne également d'autres droits et libertés fondamentaux et tous les types de données *indépendamment* de leur rapport avec la vie privée, et *plus limitée*, en ce qu'elle ne concerne que le traitement des données à caractère personnel et qu'il n'est pas tenu compte des autres dimensions de la protection de la vie privée.

Dans ce contexte, il convient de souligner qu'aujourd'hui, de nombreuses activités du secteur public ou du secteur privé sont liées d'une façon ou d'une autre à la collecte et au traitement de données à caractère personnel. L'objectif réel de la Convention consiste donc à protéger les personnes physiques (citoyens, consommateurs, travailleurs, etc.) contre la collecte, l'enregistrement, l'utilisation et la diffusion injustifiés de données les concernant. Il peut également s'agir de leur participation aux relations sociales, en public ou non, de protéger la liberté d'expression, d'empêcher la discrimination injustifiée et de promouvoir un «traitement

[8] La première législation nationale a été adoptée en Suède, en 1972. Le land allemand de la Hesse a adopté la première loi sur la protection de la vie privée au monde en 1971. Les États-Unis ont également joué un rôle majeur à ce stade avec la formulation de «principes équitables de traitement de l'information», qui ont eu une grande influence sur le débat international. Voir le rapport «*Records, Computers and the Rights of Citizens*», ministère de la santé, de l'éducation et du bien-être des États-Unis, 1973, et la loi sur la protection de la vie privée adoptée en 1974.

[9] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, STE nº 108.

[10] L'Uruguay a été le premier pays tiers à ratifier la Convention en avril 2013.

[11] Article premier.

[12] Article 2, point a.

équitable» dans les processus décisionnels. Enfin, la Convention visait également à concilier le respect de la vie privée et la libre circulation des informations.[13]

C. Garanties structurelles

La Convention énonce une série de principes de base régissant la protection des données, auxquels chaque partie doit avoir donné effet dans son droit interne avant l'entrée en vigueur de la Convention à son égard.[14] Ces principes continuent de former le noyau de toute législation nationale dans ce domaine. Aux termes de la Convention, les données à caractère personnel doivent être «obtenues et traitées loyalement et licitement», «enregistrées pour des finalités déterminées et légitimes et ne pas [être] utilisées de manière incompatible avec ces finalités». Elles doivent également être «conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées». Par ailleurs, les données à caractère personnel doivent être «adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées» et «exactes et si nécessaire mises à jour».[15]

La Convention prévoit des conditions plus rigoureuses pour les «catégories particulières de données».[16] Conformément à la disposition pertinente, les «données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle» ne peuvent être traitées à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même pour les données à caractère personnel concernant des condamnations pénales.

D'autres principes de base de la Convention exigent des «mesures de sécurité appropriées»[17] et «des garanties complémentaires pour la personne concernée», comme le droit d'obtenir la communication des données à caractère personnel la concernant, le droit d'obtenir, le cas échéant, la rectification de ces données ou leur effacement, et le droit de disposer d'un recours si ces droits ne sont pas respectés.[18] Le principe de «contrôle indépendant» ne figurait pas dans la Convention à l'origine, ce qui n'a pas empêché qu'il soit appliqué massivement dans la pratique, puis ajouté à la Convention sous la forme d'un protocole.[19]

[13] Préambule, paragraphe 4
[14] Article 4.
[15] Article 5.
[16] Article 6.
[17] Article 7.
[18] Article 8.
[19] Le protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, Strasbourg, 8 novembre 2001; voir notamment l'article 1er. Cela était principalement dû aux dispositions pertinentes de la directive 95/46/CE (voir la section 3, partie B, ci-dessous).

Soyons bien clairs: l'approche de la Convention ne consiste *pas* à considérer systématiquement le traitement des données à caractère personnel comme une *atteinte* au droit à la vie privée, mais prévoit que, pour assurer la *protection* de la vie privée et d'autres droits et libertés fondamentaux, tout traitement de données à caractère personnel doit *toujours* respecter certaines conditions juridiques, comme le principe suivant lequel les données à caractère personnel ne peuvent être traitées qu'à des fins légitimes et spécifiées, si ce traitement est bien nécessaire à ces fins, et qu'elles ne peuvent être utilisées d'une manière incompatible avec les fins qui justifient leur traitement.

Conformément à cette approche, la substance de l'article 8 de la CEDH, qui est de limiter le droit d'ingérence dans la vie privée aux cas exclusifs où une base juridique adéquate le justifie et où une finalité légitime le requiert, a donc été appliquée à un contexte plus large. En outre, selon les dispositions de la Convention, aucune dérogation à ces principes n'est autorisée, à l'exception de ce qui est déjà applicable au droit à la vie privée lui-même.[20]

Précisons que cela ne fonctionne bien dans la pratique que si le système de poids et contrepoids prévu par la Convention - composé de certaines conditions matérielles, de droits individuels, de dispositions visant à garantir une procédure conforme et un contrôle indépendant - est suffisamment flexible pour tenir compte de la variabilité des contextes et est appliqué avec pragmatisme, tout en tenant compte des intérêts des personnes concernées et des autres parties intéressées. Dans cette perspective, le droit au respect de la vie privée tel qu'il est prévu à l'article 8 de la CEDH continue de jouer un rôle important en toile de fond, entre autres afin de déterminer la légitimité de certaines mesures particulières plus intrusives.

La Convention a joué un rôle majeur dans l'orientation suivie par les législateurs de la plupart des États membres du Conseil de l'Europe. À cet égard, la question de la «protection des données» a été considérée dès le départ comme un sujet de grande importance structurelle pour les sociétés modernes, où le traitement des données à caractère personnel occupe une place de plus en plus importante. La Convention est également en cours de révision actuellement et nous reviendrons brièvement sur ce sujet ultérieurement.

D. Autres aspects

Après l'adoption de la Convention 108, le Conseil de l'Europe a conservé un rôle actif au travers l'élaboration d'une série de recommandations du Comité des ministres au sujet de l'application de la Convention dans différents secteurs, ce qui a permis de clarifier

[20] Article 9.

considérablement plusieurs dispositions clés.[21] Ces recommandations ont ouvert la voie aux législations nationales et fourni des points de repère utiles pour d'autres accords internationaux.[22]

À l'époque, les dispositions de la Convention n'étaient pas destinées à s'appliquer directement ou à être incluses dans le contrôle judiciaire de la CEDH. Depuis 1997, la Cour européenne des droits de l'homme a cependant statué dans plusieurs d'affaires que la protection des données à caractère personnel revêt une «importance fondamentale» pour la jouissance du droit au respect de la vie privée, tel que garanti par l'article 8 de la CEDH, et a tiré de la Convention des critères lui permettant de déterminer dans quelle mesure ce droit avait été violé.[23] La Cour semble de plus en plus encline à apprécier le respect de la Convention - en tout cas pour les «données sensibles» - dans le cadre de l'article 8 de la CEDH.

Cela nous mène également à la question de savoir dans quelle mesure les lacunes de l'article 8 de la CEDH qui ont conduit à l'adoption de la Convention existent encore. La notion de «vie privée» au sens de l'article 8 n'est toujours pas tout à fait claire, mais sa portée s'est fortement élargie.[24] Selon la jurisprudence de la Cour européenne des droits de l'homme, la vie privée ne se limite pas aux situations «intimes», mais couvre également certains aspects de la vie professionnelle et le comportement en public, par le passé ou non. D'autre part, ces cas de figure concernent encore souvent des situations spécifiques, qui impliquent des informations sensibles (services médicaux ou sociaux), des attentes légitimes en matière de respect de la vie privée (utilisation confidentielle du téléphone ou du courrier électronique au travail) ou les enquêtes menées par les services de police ou de renseignement. Jusqu'à présent, la Cour n'a jamais statué que *tout* traitement de données à caractère personnel - *indépendamment* de sa nature ou de son contexte - relève du champ

[21] À titre d'exemple, la recommandation nº R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques, en son point 1.2, a clarifié la notion de «donnée à caractère personnel» en affirmant qu'une personne physique n'est pas considérée comme «identifiable» si cette identification nécessite des délais, des coûts et des activités déraisonnables. Le rapport explicatif de la Convention indiquait de façon plutôt ambiguë qu'une «personne identifiable» était une personne pouvant être «facilement identifiée» et que «cela ne couvre pas l'identification de personnes par des méthodes très complexes» (point 28).

[22] La recommandation nº (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police a servi de référence pour établir le niveau de protection vis-à-vis d'Europol [voir article 14 de la Convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de police (convention Europol) et le considérant 14 de l'actuelle décision du Conseil portant création d'Europol (2009/371/JAI)].

[23] Voir, par exemple, l'arrêt de la Cour européenne des droits de l'homme, *Z c. Finlande*, requête nº 22009/93, CEDH 1997-I, point 95.

[24] Voir, par exemple, les arrêts de la Cour européenne des droits de l'homme, *Klass c. Allemagne*, CEDH 1978, série A, nº 28; *Malone c. Royaume-Uni*, CEDH 1984, série A, nº 82; *Leander c. Suède*, CEDH 1987, série A, nº 116; *Gaskin c. Royaume-Uni*, CEDH 1989, série A, nº 160; *Niemietz c. Allemagne*, CEDH 1992, série A, nº 251-B; *Halford c. Royaume-Uni*, CEDH 1997-IV; *Amann c. Suisse*, CEDH 2000-II, et *Rotaru c. Roumanie*, CEDH 2000-V.

d'application de l'article 8.[25] Dès lors, la Convention ne constitue qu'une source additionnelle de critères pour évaluer la conduite dans le cadre de cette disposition.

Désormais, la Cour a également jugé que l'article 8 de la CEDH peut entraîner des obligations positives à charge des États membres et que la responsabilité de ces derniers peut par conséquent être mise en cause pour une violation de la vie privée commise par un particulier.[26] Néanmoins, le nombre d'affaires pertinentes reste limité et n'équivaut pas à une obligation générale pour les États membres de garantir la protection des données à caractère personnel dans les relations horizontales. La Convention continue donc de jouer un rôle complémentaire utile à cet égard.

Quelques années à peine après l'adoption de la Convention 108, la Cour constitutionnelle allemande a rendu une décision dans laquelle elle définissait un droit à «l'autodétermination en matière d'informations» comme traduisant le droit au libre épanouissement de la personnalité consacré à l'article 2, paragraphe 1, de la Constitution allemande.[27] Dans cette optique, tout traitement de données à caractère personnel est en principe considéré comme une ingérence dans le droit à l'autodétermination en matière d'informations, à moins que la personne concernée y ait consenti. Cette décision a eu une forte influence, non seulement en Allemagne, mais également ailleurs en Europe. Cependant, il convient de bien distinguer l'approche adoptée dans la Convention 108 et, sur cette base - comme nous le verrons - celle de la directive 95/46/CE et les dispositions pertinentes de la charte de l'Union.

Quelques mois avant l'adoption de la Convention 108, l'OCDE a adopté ses lignes directrices régissant la protection de la vie privée qui, bien qu'elles ne soient pas contraignantes, ont également eu une influence considérable, notamment dans des pays situés en dehors de l'Europe, comme les États-Unis, le Canada, l'Australie et le Japon.[28] Ces lignes directrices contenaient un ensemble de principes fondamentaux rédigés en étroite coordination avec le Conseil de l'Europe et étaient donc cohérentes avec les principes de la Convention 108 en

[25] Malgré un discours parfois ambigu, par exemple dans l'arrêt du 18 octobre 2011, *Khelili c. Suisse*, requête nº 16188/07, au point 56: «la mémorisation de données *relatives à la vie privée de la requérante*, dont fait partie la profession, et leur conservation, constituent une ingérence au sens de l'article 8 de la Convention, *car il s'agit d'une donnée à caractère personnel se rapportant à un individu identifié ou identifiable*» (italique ajouté). Soulignons toutefois que cette affaire portait sur la conservation, par la police pendant une longue période et sans fondement factuel suffisant, de données incluant une référence à la requérante en tant que prostituée. Dans le même arrêt, la Cour a en outre fait valoir que pour déterminer si les informations à caractère personnel conservées font entrer en jeu l'un des aspects de la vie privée, il convient de tenir compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés (voir point 55).

[26] Voir, par exemple, les arrêts de la Cour européenne des droits de l'homme, *von Hannover c. Allemagne*, CEDH 2004-VI, et *K.U. c. Finlande*, requête nº 2872/02, CEDH 2008-V.

[27] Arrêt du 15 décembre 1983, BVerfGE 65, 1-71, *Volkszählung.*

[28] Recommandation du conseil de l'OCDE concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, Paris, le 23 septembre 1980, disponible à l'adresse suivante: http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm (dernière consultation le 31 mai 2014)

matière de protection des données. Des différences plutôt subtiles, mais significatives, ont été observées sur des détails. Le champ d'application des lignes directrices était limité aux données à caractère personnel «qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles».[29] Cette définition comporte la notion de «risque» comme condition *minimale* de protection, une condition qui n'était pas tout à fait compatible avec l'approche basée sur les droits fondamentaux suivie par le Conseil de l'Europe. De plus, la nécessité d'une finalité *légitime* et de la *licéité* du traitement de données à caractère personnel en tant que telles ne figurait pas dans les lignes directrices.[30] Ces deux points sont liés à des problèmes qui revêtent toujours une grande importance dans les forums mondiaux.

3. Directive 95/46/CE

A. Harmonisation

Bien que le Conseil de l'Europe ait très bien réussi à mettre la question de la «protection des données» à l'ordre du jour et à définir les principaux éléments d'un cadre juridique, il a moins bien réussi à assurer une cohérence suffisante parmi ses États membres. Certains États membres ont tardé à mettre la Convention 108 en œuvre, tandis que d'autres qui l'ont fait ont obtenu des résultats plutôt variables et ont même, dans certains cas, imposé des restrictions sur les flux de données vers les autres États membres.

La Commission européenne a donc craint que ce manque de cohérence n'entrave le développement du marché intérieur dans une série de domaines - impliquant la libre circulation des personnes et des services - dans lesquels le traitement des données à caractère personnel était appelé à jouer un rôle de plus en plus important. Fin 1990, elle a donc présenté une proposition de directive visant à harmoniser les législations nationales sur la protection des données dans le secteur privé et dans la plus grande partie du secteur public. [31]

À l'issue de quatre années de négociations, la directive 95/46/CE[32] actuellement en vigueur a été adoptée avec un double objectif. Tout d'abord, elle exige de tous les États membres qu'ils assurent, conformément à ses dispositions, la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement

[29] Lignes directrices, paragraphe 2.
[30] Voir les lignes directrices, paragraphe 7: «toute donnée de ce type devrait être obtenue par des *moyens licites et loyaux* et, *le cas échéant*, après en avoir informé la personne concernée ou avec son consentement» (italique ajouté).
[31] COM (90) 314 final - SYN 287 et 288, 13 septembre 1990, page 4: «La diversité des approches nationales et l'absence d'un système de protection au niveau communautaire constituent un obstacle à l'achèvement du marché intérieur. Si les droits fondamentaux des personnes concernées, en particulier leur droit à la vie privée, ne sont pas protégés au niveau communautaire, la circulation transfrontalière des données pourrait être entravée [...]».
[32] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données; JO L 281 du 23.11.1995, p. 31.

des données à caractère personnel. En deuxième lieu, elle prévoit qu'ils ne peuvent ni restreindre ni interdire la libre circulation des données à caractère personnel entre les États membres pour des raisons afférentes à cette protection.[33] Ces deux obligations sont étroitement liées entre elles. Elles visent à créer un niveau de protection élevé équivalent dans l'ensemble des États membres en vue d'obtenir un développement équilibré du marché intérieur.

À cet égard, la directive est partie des principes de base de la protection des données, tels qu'énoncés dans la Convention 108 du Conseil de l'Europe.[34] En même temps, elle précisait ces principes et les complétait par d'autres exigences et conditions. Cependant, comme la directive recourait à des concepts formulés de manière générale et à des normes ouvertes, elle laissait tout de même une marge d'appréciation assez large aux États membres pour sa transposition.[35] Il en a résulté que la directive a permis d'obtenir une meilleure cohérence entre les États membres, mais certainement pas de parvenir à des solutions identiques ou parfaitement cohérentes.

B. Portée et contenu

Le champ d'application de l'actuelle directive est vaste: elle s'applique à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier[36]. Deux exceptions à cela: tout d'abord, le traitement en dehors du champ d'application du droit communautaire, désormais devenu droit de l'Union, et, en tout état de cause, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État ou l'application du droit pénal et, deuxièmement, les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.[37] Les définitions apportées aux termes tels que «traitement» et «données à caractère personnel» sont très proches de celles de la Convention 108.[38]

La directive applique également les principes fondamentaux de la protection des données consacrés par la Convention, mais ajoute six critères de légitimité du traitement des données qui ne sont pas précisés dans la Convention.[39] Le traitement des données à caractère

[33] Voir les considérants 7 à 10, et l'article 1er.
[34] Voir notamment le considérant 11.
[35] Voir le considérant 9 et l'article 5.
[36] Article 3, paragraphe 1.
[37] Article 3, paragraphe 2.
[38] Article 2, points a) et b). Pour plus de détails, à propos du second sujet, voir: groupe de travail «Article 29», avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007 (WP 136), disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf (dernière consultation le 31 mai 2014).
[39] Article 7. Voir à cet égard l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement, adopté le 3 juillet 2011 (WP 187), ainsi que l'avis 6/2014 sur la notion d'intérêt légitime du responsable du traitement en vertu de l'article 7 de la directive 95/46/CE, adopté le 9 avril 2014 (WP 217), disponibles aux adresses suivantes:

personnel n'est autorisé que si la personne concernée a *indubitablement* donné son consentement, ou s'il est *nécessaire* à l'exécution d'un contrat auquel la personne concernée est partie, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public, à la sauvegarde de l'intérêt vital de la personne concernée ou à la protection de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévale pas l'intérêt de la personne concernée. Un examen subtil des différentes phases du traitement des données est donc nécessaire et les responsables du traitement doivent tenir compte de cette analyse en temps opportun.

La directive précise également les conditions qui régissent le traitement de catégories particulières de données sensibles.[40] Le point de départ est une *interdiction* assortie de certaines exceptions, moyennant soit le consentement *explicite* de la personne concernée, soit le respect de conditions particulières, notamment pour le traitement de données relatives à la santé en matière de soins. D'autres exceptions peuvent être prévues à l'échelon national, mais uniquement pour «un motif d'intérêt public important» et «sous réserve de garanties appropriées». La directive prévoit la notification des dérogations à la Commission afin d'assurer un recours limité à cette option.

Un autre élément de la directive est l'obligation pour le responsable du traitement de fournir à la personne concernée, sauf si elle en dispose déjà, des informations adéquates sur son identité, les finalités du traitement et les autres informations pertinentes, pour autant que «compte tenu des circonstances particulières dans lesquelles les données sont collectées», ces informations supplémentaires sont «nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données».[41] Le défaut de transparence à cet égard peut rendre la collecte des données illégale, avec toutes les conséquences qui en résulteront.

La directive prévoit en outre la mise en place d'autorités de contrôle chargées de surveiller la conformité des législations nationales sur leur territoire respectif, autorités qui seront investies d'un certain nombre de missions et de compétences spéciales, qu'elles sont tenues d'exercer «en toute indépendance».[42] Ces missions peuvent comprendre des contrôles préalables ou une consultation[43], le traitement des réclamations, des inspections et autres activités de répression, en fonction de la manière dont la directive a été mise en œuvre en droit interne. Ces autorités coopèrent dans l'exercice de leurs fonctions, soit bilatéralement,

---

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf (dernière consultation le 31 mai 2014)
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf (dernière consultation le 31 mai 2014)

[40] Article 8.
[41] Articles 10 et 11.
[42] Article 28.
[43] Articles 18 à 20.

soit dans le cadre du groupe de travail «Article 29», qui revêt un caractère consultatif et indépendant au niveau de l'UE.[44]

Sur le plan territorial, la directive s'applique au traitement de données à caractère personnel effectué «dans le cadre des activités d'un établissement» du responsable du traitement sur le territoire de l'un des État membres de l'UE.[45] Le lieu où les données sont traitées n'est pas pertinent à cet égard. Ce critère est également décisif pour la portée de la législation nationale au sein de l'UE. Si le responsable du traitement 'n'est pas établi dans l'UE, le droit applicable est celui de l'État membre dans lequel les moyens utilisés aux fins de traitement des données sont localisés.[46]

La directive consacre également le principe selon lequel les données à caractère personnel ne peuvent être transférées que vers des pays tiers qui garantissent un niveau de protection adéquat, à défaut de quoi le transfert n'est autorisé que dans certaines situations: soit sur la base d'une exception, soit lorsque des garanties suffisantes ont été apportées contractuellement ou par tout autre instrument pertinent.[47]

Ces dispositions s'appliquent aujourd'hui à une réalité complexe dans laquelle la question de savoir quel droit est applicable et qui est responsable de son application se pose de plus en plus souvent, tant au sein de l'UE que par rapport aux pays tiers. Cela soulève également de nouvelles questions concernant l'internet - au sujet de la position des sites web, des moteurs de recherche[48], des réseaux sociaux et des techniques de publicité modernes - et les flux de données au sein des entreprises multinationales, la sous-traitance des services et l'informatique en nuage. Dans la pratique, une protection adéquate est de plus en plus souvent assurée par des «règles d'entreprise contraignantes», des codes de conduite adoptés par les entreprises, qui satisfont à des exigences spécifiques et sont considérés comme suffisamment efficaces par les contrôleurs compétents.[49]

---

[44] Articles 29 et 30, qui font également référence au contrôleur européen de la protection des données en tant que membre dudit groupe.

[45] Article 4. Voir l'arrêt du 13 mai 2014, *Google Spain*, C-131/12, non encore publié au Recueil, points 55 et 56. Voir la section 6, partie D, ci-dessous.

[46] Pour plus de détails, voir l'avis 8/2010 du groupe de travail «Article 29» sur le droit applicable, adopté le 16 décembre 2010 (WP 179), disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_fr.pdf (dernière consultation le 31 mai 2014)

[47] Articles 25 et 26. Sur cette base, la Commission européenne a reconnu un certain nombre de pays tiers comme appliquant un niveau de protection suffisant et a approuvé les clauses contractuelles pouvant garantir une protection suffisante dans des cas particuliers. Pour plus d'informations, veuillez consulter le site web de la Commission européenne et du groupe de travail «Article 29» à l'adresse suivante: http://ec.europa.eu/justice/data-protection/index_fr.htm (dernière consultation le 31 mai 2014)

[48] Voir l'arrêt *Google Spain*, cité à la note de bas de page 45, selon lequel l'exploitant du moteur de recherche est le responsable du traitement et doit veiller au respect de la législation européenne sur la protection des données (points 33 et 38). Voir la section 6, partie D, ci-dessous.

[49] L'article 26, paragraphe 2, indique que ces garanties suffisantes peuvent «notamment» résulter de clauses contractuelles appropriées, mais n'exclut pas d'autres instruments. De plus amples informations sur les règles d'entreprise contraignantes sont disponibles sur le site web mentionné à la note de bas de page 44.

La nécessité de concilier le respect de la vie privée et la libre circulation des informations – l'un des objectifs de la Convention 108 qui ressort également des objectifs de la directive - a finalement abouti à une disposition plus spécifique imposant aux États membres de prévoir des exemptions et des dérogations potentiellement très étendues à certaines dispositions pour les traitements de données à caractère personnel «effectués aux seules fins de journalisme ou d'expression artistique ou littéraire», dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.[50]

C. Jurisprudence pertinente

Tous les États membres de l'Union ont transposé la directive dans leur législation nationale, y compris les nouveaux États membres pour qui cette transposition était une condition d'adhésion et les membres de l'EEE qui ne font pas partie de l'Union. La Commission a déjà également intenté plusieurs actions en justice pour mise en œuvre inadéquate de la directive. La première mettait en cause l'État membre ayant la plus longue expérience dans ce domaine: l'Allemagne. En mars 2010, la Cour de justice de l'Union européenne a décidé que l'exigence d'une «indépendance complète» signifie qu'une autorité de contrôle doit être exempte de *toute* influence extérieure.[51] Cette position a été confirmée plus récemment et développée dans deux procédures intentées contre l'Autriche et la Hongrie.[52]

D'autres arrêts importants ont également été rendus par la Cour de justice sur d'autres aspects de l'actuel cadre juridique pour la protection des données à caractère personnel. Ainsi, la Cour a, dans ses premiers arrêts concernant la directive 95/46/CE, jugé que celle-ci possède un champ d'application très large qui ne dépend pas, dans chaque affaire, d'un lien direct avec le marché intérieur.[53] En d'autres termes, la directive s'applique aussi bien à un litige dans le secteur public d'un État membre donné qu'au site web d'une institution ecclésiastique ou caritative. Dans ce dernier cas, il a également été précisé que la directive s'applique en principe à l'internet, même si le simple fait que des données à caractère personnel sont disponibles sur un site web n'implique pas automatiquement que les dispositions régissant les flux de données avec les pays tiers s'appliquent.[54] Les conséquences précises de cette conclusion ne sont pas tout à fait claires.

Lorsque la directive s'applique à un domaine relevant de l'article 8 de la CEDH, elle doit être interprétée en tenant compte de cette disposition.[55] Dans ce contexte, la Cour a opéré une

[50] Article 9.
[51] Arrêt rendu dans l'affaire *Commission/Allemagne*, C-518/07, Rec. 2010, p. I-01885, point 30.
[52] Arrêt du 16 octobre 2012, *Commission/Autriche*, C-614/10, et arrêt du 8 avril 2014, *Commission/Hongrie*, C-288/12, aucun des deux n'étant encore publié au Recueil.
[53] Voir les arrêts rendus dans les affaires jointes *Österreichischer Rundfunk*, C-465/00, C-138/01 et C-139/01, Rec. 2003, p. I-04989, points 41 à 43, et dans l'affaire *Bodil Lindqvist*, C-101/01, Rec. 2003, p. I-12971, points 39 à 41.
[54] Arrêt *Bodil Lindqvist*, précité, points 24 à 27 et 56 à 71.
[55] Arrêt *Österreichischer Rundfunk*, points 68 à 72.

distinction entre les traitements de données susceptibles - ou non - de violer l'article 8 de la CEDH. Les premiers concernaient une législation nationale qui obligeait les employeurs à fournir à un organisme public certaines données concernant les revenus de leurs salariés. Le traitement de ces données par l'employeur lui-même à des fins professionnelles ne posait en principe pas de problème, tant que les règles de la protection des données étaient respectées.[56] Cette approche cadre bien avec la distinction entre «vie privée» et «protection des données» dans l'évolution du droit, comme cela a été indiqué précédemment.

La Cour a fait valoir l'exception prévue pour le traitement des données concernant la sécurité publique et l'application du droit pénal dans une affaire importante ayant trait au transfert de données de passagers aériens aux États-Unis aux fins de la protection des frontières à la suite des attentats terroristes du 11 septembre 2001.[57] Dans d'autres affaires, la Cour a jugé que l'exception relative au traitement des données par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques vise uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est clairement pas le cas des données à caractère personnel rendues accessibles à un nombre indéfini ou illimité de personnes.[58] Dans l'une de ces affaires, la Cour a également statué que l'exception accordée pour le traitement aux fins du journalisme devait être appliquée largement, de manière à inclure toutes les activités ayant pour unique finalité la divulgation au public d'informations, d'opinions ou d'idées.[59]

Dans une affaire ayant trait aux critères applicables en ce qui concerne la légitimité d'un traitement de données, la Cour a jugé que l'Espagne n'avait pas transposé correctement l'article 7, point f), de la directive, en exigeant qu'en l'absence de consentement de la personne concernée, toutes les données faisant l'objet d'un traitement devaient figurer dans des sources accessibles au public.[60] La Cour a également jugé que l'article 7, point f), avait un effet direct.[61] L'arrêt limite la marge de discrétion dont les États membres jouissent dans la mise en œuvre de l'article 7, point f). Plus particulièrement, ils ne doivent pas franchir la ligne mince qui sépare la précision ou la clarification, d'une part, et l'imposition d'exigences additionnelles, qui modifieraient le champ d'application de l'article 7, point f), d'autre part.

Dans une affaire portant sur l'étendue du droit d'accès aux registres automatisés de la population aux Pays-Bas, la Cour a jugé que les États membres étaient tenus de garantir un

[56] Arrêt *Österreichischer Rundfunk*, points 73 et 74.
[57] Arrêt rendu dans les affaires jointes, *PNR*, C-317/04 et C-318/04, Rec. 2006, p. I-04721, points 56 à 59 et 67 à 69. Pour une analyse critique de cet arrêt, voir: Docksey, C., «The European Court of Justice and the Decade of Surveillance», dans Hijmans, H., et Kranenborg, H., (ed.), *Data Protection Anno 2014: How to Restore Trust?*, 2014, pages 97 à 111.
[58] Arrêt *Bodil Lindqvist*, précité, points 46 et 47, et arrêt rendu dans l'affaire *Satamedia*, C-73/07, Rec. 2008, p. I-09831, points 43 et 44.
[59] Arrêt *Satamedia*, points 56 et 61.
[60] Arrêt rendu dans les affaires jointes *ASNEF*, C-468/10 et C-469/10, Rec. 2011, p. I-12181, points 32 à 39 et 49.
[61] Arrêt *ASNEF*, points 51 à 54.

droit d'accès aux informations concernant les traitements effectués, notamment sur les destinataires des données à caractère personnel et sur le contenu des données divulguées par le passé. Il appartient aux États membres de fixer une limite temporelle pour le stockage de ces informations et d'en assurer l'accès, ce qui constitue un juste équilibre entre, d'une part, l'intérêt de la personne concernée à voir sa vie privée protégée et, d'autre part, le poids que représente, pour le responsable du traitement, l'obligation de stocker ces informations. Cependant, les règles qui limitent le stockage des informations relatives au traitement à un an, alors que les données de base sont elles-mêmes conservées pendant une période beaucoup plus longue, ne sont pas de nature à assurer un juste équilibre entre l'intérêt et l'obligation en question, à moins qu'un stockage de plus longue durée ne fasse peser une charge excessive sur le responsable du traitement.[62] Cet arrêt démontre un entendement clair du rôle essentiel du droit d'accès de la personne concernée et de l'environnement complexe dans lequel il peut être amené à être exercé dans la pratique.

4. Aspects institutionnels

A. Autres instruments

Jusqu'à présent, nous nous sommes concentrés sur la directive 95/46/CE, mais ce n'est pas le seul instrument pertinent de la législation européenne en matière de protection des données. Il existe au moins trois autres catégories d'instruments, qu'il convient d'aborder brièvement: les actes qui précisent les règles dans un domaine particulier, ceux qui appliquent les règles à l'échelon de l'Union et ceux qui les appliquent dans le domaine répressif. Un exemple de la première catégorie est la directive 2002/58/CE sur la vie privée et les communications électroniques, qui est venue préciser la directive 95/46/CE en ce qui concerne les services de communications électroniques accessibles au public et les réseaux de communication publics.[63] Elle traite de questions allant de la sécurité et la confidentialité des communications au stockage et à l'utilisation des données relatives à la circulation et à la localisation, ainsi qu'aux communications non sollicitées, indépendamment de la technologie utilisée. Bien que la directive s'applique donc également à l'internet, elle demeure limitée à son propre champ d'application. Certains traitements de données importants effectués dans le cadre de sites web relèvent toujours du champ d'application de la directive 95/46/CE.[64]

Un exemple de la deuxième catégorie est le règlement (CE) nº 45/2011, qui a mis en œuvre les directives 95/46/CE et 97/66/CE (à laquelle a succédé la directive 2002/58/CE) pour les

[62] Arrêt rendu dans l'affaire *Rijkeboer*, C-553/07, Rec. 2009, p. I-03889, points 56 à 70.

[63] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201 du 31.7.2002, p. 37 (directive «Vie privée et communications électroniques»). Voir notamment l'article 1er sur le champ d'application et l'objectif de la directive.

[64] Voir, par exemple, les arrêts *Lindqvist* et *Google Spain*.

institutions et les organes de l'Union européenne.[65] L'article 286 du traité CE, adopté en 1997 dans le cadre du traité d'Amsterdam, prévoyait que les «actes communautaires» relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données devaient également s'appliquer à l'échelon de l'Union européenne et posait la base juridique de la création d'une autorité de contrôle indépendante. Cela n'aurait pas été possible sans une base juridique aussi particulière. Le règlement (CE) nº 45/2001 établit un ensemble complet de règles dans un seul instrument et institue le contrôleur européen de la protection des données en lui conférant un certain nombre de tâches et de pouvoirs fondés sur ceux définis dans la directive 95/46/CE.[66]

La troisième catégorie est légèrement différente. Jusqu'à présent, nous avons essentiellement abordé la base juridique du marché intérieur dans ce qui était le «premier pilier» de l'Union européenne. Manifestement, celle-ci ne s'appliquait pas aux autres piliers, à savoir la politique étrangère et de sécurité commune («deuxième pilier») et la coopération policière et judiciaire en matière pénale («troisième pilier»), qui ont été introduit par le traité de Maastricht en 1992. Le traité d'Amsterdam a transféré certains domaines couverts par le troisième pilier - comme l'immigration, l'asile et le contrôle des frontières - vers le premier pilier, rassemblant ainsi ces domaines dans le champ d'application de la directive 95/46/CE. Quelques règlements revêtant une importance particulière au regard de la protection des données ont été adoptés dans ce contexte.[67]

Les dispositions du troisième pilier du traité sur l'Union européenne contenaient toutefois certaines bases juridiques spécifiques pour la législation sur la protection des données. Selon l'approche suivie dans ce contexte, l'action commune dans le domaine de la coopération policière ou de la coopération judiciaire en matière pénale devait faire l'objet de garanties appropriées concernant la protection des données à caractère personnel, et des normes communes en matière de protection des données pouvaient également contribuer à garantir l'efficacité et la légitimité de la coopération.[68] Cette optique a conduit à l'adoption de plusieurs décisions sur des sujets spécifiques, dont Eurojust et Europol[69], ainsi qu'en 2008, à

[65] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 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 (JO L 8 du 12.1.2001, p. 1).

[66] Voir les articles 41 à 48 sur le CEPD. Ces dispositions ont servi de repère dans les arrêts de la Cour de justice sur l'indépendance des autorités de contrôle (voir les notes de bas de page 51 et 52, et notamment l'affaire *Commission/Allemagne*, points 26 à 28).

[67] Par exemple, le règlement (CE) nº 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, JO L 316 du 15.12.2000, p. 1 (voir notamment les considérants 15 à 17), et le règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), JO L 218 du 13.8.2008, p. 60 (voir notamment les considérants 17 à 20, mentionnant également les contrôles coordonnés par les autorités nationales de la protection des données et le CEPD).

[68] Voir les articles 30 et 31 du TUE, avant l'entrée en vigueur du traité de Lisbonne.

[69] Décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité,

la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 contenant des règles générales sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.[70] Le contenu de ces règles s'inspirait de la directive 95/46/CE et de la Convention 108 du Conseil de l'Europe, mais le niveau de protection était nettement moindre en termes de champ d'application et de substance.[71] En ce qui concerne le champ d'application, la décision ne s'applique que lorsque les données à caractère personnel sont transmises ou mises à la disposition d'autres États membres, et ne couvre dès lors pas le traitement dans un contexte «national», contrairement à la directive 95/46/CE.[72]

B. La charte des droits fondamentaux

Les droits fondamentaux garantis par la Convention européenne des droits de l'homme ou résultant des traditions constitutionnelles communes aux États membres ont longtemps été reconnus et appliqués par la Cour de justice de l'Union européenne en tant que principes généraux de droit européen. En juin 1999, le Conseil européen a néanmoins décidé qu'il était temps d'établir une charte des droits fondamentaux de l'Union européenne «afin d'ancrer l'importance exceptionnelle et la portée des droits fondamentaux de manière visible pour les citoyens de l'Union».[73] Cette décision a abouti, en décembre 2000, lors du sommet européen de Nice, à la proclamation de la charte des droits fondamentaux de l'Union européenne, qui n'était à l'origine qu'un document politique.[74]

Un des éléments novateurs de la charte était qu'*outre* le droit au respect de la vie privée, elle reconnaissait également de manière explicite le droit à la protection des données à caractère personnel dans une disposition distincte. L'article 7 relatif au «*[r]espect de la vie privée et familiale*» dispose que «toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications». L'article 8, concernant la «*[p]rotection des données à*

JO L 138 du 4.6.2009, p. 14, et décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol), JO L 121 du 15.5.2009, p. 37.

[70] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60.

[71] Voir l'évaluation faite par la Commission elle-même au moment d'expliquer la nécessité de remplacer la décision (voir notes de bas de page 124, 128 et 133).

[72] Voir notamment le considérant 7 et l'article 1er.

[73] Conseil européen de Cologne des 3 et 4 juin 1999, conclusions de la présidence, points 44 et 45 et annexe IV. Une convention composée de 15 représentants des chefs d'État et de gouvernement, 30 représentants des parlements nationaux, 16 représentants du Parlement européen et un représentant de la Commission, présidée par M. Roman Herzog, ancien président de la République fédérale d'Allemagne et de la Cour constitutionnelle allemande, a été instaurée pour élaborer la charte.

[74] Charte des droits fondamentaux de l'Union européenne, JO C 364 du 18.12.2000, p. 1. La charte a été proclamée solennellement par le Parlement européen, le Conseil et la Commission, qui se sont engagés à la respecter dans le cadre de leurs activités. Le préambule met en exergue le fait que la charte est le reflet de «*valeurs communes*» et «réaffirme [...] les droits qui résultent notamment des traditions constitutionnelles et des obligations internationales *communes aux États membres*, du traité sur l'Union européenne et des traités communautaires, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [...], ainsi que de la jurisprudence de la Cour de justice des Communautés européennes et de la Cour européenne des droits de l'homme» (italique ajouté).

caractère personnel», prévoit dans son premier paragraphe que «[t]oute personne a droit à la protection des données à caractère personnel la concernant». Le deuxième paragraphe ajoute que «[c]es 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» et que «[t]oute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification». En son troisième paragraphe, l'article dispose que «[l]e respect de ces règles est soumis au contrôle d'une autorité indépendante».

Conformément aux notes explicatives, les droits garantis à l'article 7 de la charte correspondent à ceux garantis par l'article 8 de la CEDH.[75] Tous deux sont des exemples typiques de droits fondamentaux classiques, où l'*ingérence* est soumise à des conditions rigoureuses. La seule différence entre eux est que l'article 52 de la charte contient une clause d'exception plus générale.

L'explication relative à l'article 8 indique que celui-ci se fonde sur l'article 286 du traité CE et sur la directive 95/46/CE, ainsi que sur l'article 8 de la CEDH et sur la Convention 108 du Conseil de l'Europe. Elle précise également que «le droit à la protection des données à caractère personnel s'exerce dans les conditions prévues par la directive susvisée et peut être limité dans les conditions prévues par l'article 52» de la charte.[76] Cette précision pousse à s'interroger sur la nature du nouveau droit et ses différents éléments visés à l'article 8, ainsi que sur la distinction entre les conditions d'«exercice» du droit prévues par la directive 95/46/CE et les conditions de «limitation» du droit exposées à l'article 52.

Comme nous l'avons vu, le droit à la protection des données à caractère personnel a été conçu par le Conseil de l'Europe et développé dans la Convention 108 afin d'assurer une protection *proactive* des droits et libertés des personnes au regard de tout traitement de données à caractère personnel, indépendamment du fait que ce traitement constitue une atteinte au droit au respect de la vie privée ou non. Le but était de mettre en place un système d'«équilibre des pouvoirs» en vue d'offrir une protection *structurelle* aux personnes dans un large éventail de situations, aussi bien dans le secteur public que privé.

[75] Explications relatives à la charte des droits fondamentaux de l'Union européenne, document CONVENT 49 du 11.10.2000, explication sur l'article 7. Le Bureau de la Convention a élaboré ces explications pour chacun des articles de la charte. Elles étaient destinées à en clarifier les dispositions en indiquant les sources et le champ d'application de chacun des droits qui y sont consacrés. Au départ, elles ne revêtaient aucune valeur juridique et n'avaient été publiées qu'à titre purement informatif. Cependant, le troisième alinéa de l'article 6, paragraphe 1, du TUE a modifié leur statut. Une version légèrement révisée a été publiée au Journal officiel (JO C 303 du 14.12.2007, p. 17) et mentionnée dans le préambule de la version finale de la charte (JO C 303 du 14.12.2007, p. 1). Voir également les publications ultérieures de la charte dans le JO C 83 du 30.3.2010, p. 389 et le JO C 326 du 26.10.2012, p. 391.

[76] Voir note de bas de page 75, explication sur l'article 8. La version révisée a inséré un renvoi à l'article 16 du TFUE et au règlement (CE) nº 45/2001, et dispose désormais que «[l]a directive et le règlement précités contiennent des conditions et limitations applicables à l'exercice du droit à la protection des données à caractère personnel». La référence à l'article 52 a aujourd'hui disparu.

La Convention 108 a servi de point de départ à la directive 95/46/CE pour l'harmonisation des législations en matière de protection des données au sein de l'Union européenne et l'a énoncé de manières différentes,[77] ce qui faisait intervenir les principes matériels de la protection des données, les obligations incombant aux responsables du traitement, les droits des personnes concernées et la nécessité d'un contrôle indépendant en tant qu'éléments structurels principaux de la protection des données. Cependant, la nature de la protection des données en tant que système d'«équilibre des pouvoirs» pour garantir la protection à chaque fois que des données à caractère personnel sont traitées n'a pas changé. En d'autres termes, les articles 7 et 8 présentent une nature différente et doivent être clairement différenciés.[78]

La convention qui a préparé la charte avant son adoption lors du sommet de Nice avait également envisagé d'ajouter à l'article 8 un droit à l'autodétermination en matière d'informations, mais cette proposition a été rejetée. En revanche, elle a décidé d'insérer un droit à la protection des données à caractère personnel afin de préserver les principaux éléments de la directive 95/46/CE, comme l'explication le souligne brièvement.[79] Ainsi, les éléments essentiels énoncés à l'article 8, paragraphes 2 et 3, correspondent aux principes fondamentaux de la directive 95/46/CE, tels que le traitement loyal et licite, la limitation des finalités, les droits d'accès et de rectification, et l'exercice d'un contrôle indépendant. Cela suggère qu'une «limitation» du droit à la protection des données n'intervient que lorsque ces principaux éléments de la protection des données ne sont pas respectés. La directive 95/46/CE et la Convention 108 prévoient déjà certaines exceptions aux principes de base, lorsqu'elles s'avèrent nécessaires pour des motifs légitimes. La distinction entre les conditions relatives à l'«exercice» et les conditions relatives à la «limitation» du droit à la protection des données est, dès lors, déjà intégrée dans le cadre juridique actuel.

En outre, il ne peut être exclu que la Cour de justice puisse trouver d'autres éléments essentiels de la protection des données qui n'ont pas été exprimés à l'article 8, paragraphes 2 et 3, mais sont présents dans la directive 95/46/CE et peuvent être considérés comme implicites à l'article 8, paragraphe 1, de la charte. Ces éléments pourraient également

[77] Voir la section 3, parties A et B, ci-dessus.

[78] Cette position va au-delà de l'analyse réalisée par Kokott, J., et Sobotta, Ch., «The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR», dans Hijmans, H., et Kranenborg, H. (ed.), *Data Protection Anno 2014: How to Restore Trust?*, (2014), pages 83 à 95, et une version précédente dans *International Data Privacy Law*, 2013, Vol. 3, nº 4, pages 222 à 228.

[79] Voir note de bas de page 76. Il convient de noter que le groupe de travail «Article 29» a été indirectement associé aux travaux de la convention. Son vice-président (1998-2000) et président (2000-2004), le professeur Sefano Rodota, était également membre de la convention. À un premier stade, le groupe de travail a adopté une recommandation en vue d'insérer un droit fondamental à la protection des données dans la charte (voir la recommandation 4/99 concernant l'inclusion du droit fondamental à la protection des données dans le catalogue européen des droits fondamentaux, arrêtée le 7 septembre 1999 - WP 26), disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_fr.pdf). Enfin, le président de la convention, en sa qualité d'ancien président de la Cour constitutionnelle allemande, se devait de mettre en avant le droit à «l'autodétermination en matière d'informations» (voir note de bas de page 73).

contribuer à renforcer les éléments qui ont déjà été rendus explicites et à élargir l'incidence du droit général consacré à l'article 8, paragraphe 1.[80]

En tout état de cause, cela signifie qu'il convient de ne pas confondre la *portée* de l'article 8 - couvrant tous les traitements de données à caractère personnel - avec la question de savoir s'il a été *porté atteinte* au droit fondamental de l'article 8. Le simple fait que des données à caractère personnel font l'objet d'un traitement n'implique pas nécessairement une atteinte à l'article 8. Une telle violation ne peut être établie que si un ou plusieurs éléments essentiels du droit à la protection des données - comme la nécessité d'un «fondement légitime prévu par la loi» ou le «contrôle indépendant» - n'ont pas été respectés. Toute limitation du droit doit être envisagée à la lumière de l'article 52 et non se lire dans l'exigence de fondement légitime prévu par la loi visée à l'article 8, paragraphe 2. Cette exigence n'est pas une clause dérogatoire, mais un élément du droit à la protection des données lui-même. Il se peut que les auteurs de la charte n'en aient pas été pleinement conscients, mais la note explicative est parfaitement conforme à l'approche suggérée ici.[81]

C. Impact du traité de Lisbonne

L'entrée en vigueur du traité de Lisbonne en décembre 2009 a eu une incidence énorme sur l'évolution de la législation de l'Union européenne en matière de protection des données.

Tout d'abord, l'article 6, paragraphe 1, du traité sur l'Union européenne (TUE) a conféré à la charte la même valeur juridique que les traités. Elle est donc devenue un instrument contraignant non seulement pour les institutions et les organes de l'Union, mais aussi pour les États membres agissant dans le cadre du droit de l'UE.[82] Le droit à la protection des données à caractère personnel a, en outre, été énoncé spécifiquement à l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE) parmi les principes généraux de l'Union.[83] En d'autres termes, certains des principaux éléments de la directive 95/46/CE ont désormais atteint le niveau du droit primaire de l'Union européenne. Cette constatation est également pertinente au regard de la réforme en cours, comme nous le verrons ultérieurement.[84]

---

[80] Un exemple pourrait être le principe de «limitation des finalités», qui n'a été exprimé qu'en partie à l'article 8, paragraphe 2 («traitées [...] à des fins déterminées»), mais qui joue un rôle crucial dans la pratique. Pour plus de détails, voir l'avis 3/2013 du groupe de travail «Article 29» sur la limitation des finalités, adopté le 2 avril 2013 (WP 203), disponible (en anglais uniquement) à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (dernière consultation le 31 mai 2014).

[81] Voir également les légères différences entre les versions originale et révisée de l'explication sur l'article 8, telles que mises en évidence à la note de bas de page 76.

[82] Voir l'article 6, paragraphes 1 et 2, du TUE, et l'article 51 de la charte. Voir également la section 4, partie D, ci-dessous.

[83] Article 16, paragraphe 1, du TFUE: «Toute personne a droit à la protection des données à caractère personnel la concernant».

[84] Voir notamment la section 7, partie A, ci-dessous.

Deuxièmement, l'article 16, paragraphe 2, du TFUE, prévoit désormais une base juridique générale pour l'adoption de règles par le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, «relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel» par les institutions 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». Enfin, à l'instar de l'article 8, paragraphe 3, de la charte, l'article 16, paragraphe 2, du TFUE, souligne également que le respect de ces règles doit être soumis au contrôle d'autorités indépendantes.[85]

La terminologie employée dans le texte principal rappelle la directive 95/46/CE, mais le champ d'application de cette nouvelle base juridique, qui a été élevée au rang d'obligation, s'étend en réalité bien au-delà du marché intérieur et couvre en principe tous les domaines politiques de l'Union européenne.[86] Le terme «règles» permet le recours aux directives et aux règlements directement applicables, et le choix entre les deux semble maintenant être largement politique. Plus tard, nous examinerons de quelle marge d'appréciation le législateur jouit au titre de l'article 16, paragraphe 2, du TFUE, à la lumière de la charte.[87]

Troisièmement, et dans un sens beaucoup plus large, le traité de Lisbonne a également remodelé la structure institutionnelle de l'Union européenne.[88] Il a supprimé l'ancienne structure des piliers et a introduit la méthode éprouvée de l'UE pour la prise de décision également dans des domaines où l'unanimité avait été de mise au Conseil et où le Parlement ne jouait qu'un rôle consultatif. Au lieu de cela, la Commission jouait désormais son rôle habituel qui consistait à prendre l'initiative des nouvelles législations, qui devaient être adoptées par le Parlement et le Conseil au moyen de la procédure de codécision, chacun d'entre eux statuant à des majorités variables en fonction du sujet. Au terme d'une période de transition, la Cour de justice serait également à même d'exercer pleinement son rôle judiciaire et la Commission celui de gardienne des traités dans l'application du droit de l'Union européenne.[89]

---

[85] La légère différence linguistique avec l'article 8, paragraphe 3, de la charte («autorité» ou «autorités») ne semble pas avoir de conséquence.

[86] L'article 39 du TUE prévoit une base juridique spécifique pour la politique étrangère et de sécurité commune, selon laquelle «le Conseil adopte» les règles relatives à la protection des données sans l'intervention du Parlement. La déclaration 20 indique que «chaque fois que doivent être adoptées, sur la base de l'article 16, des règles [...] qui pourraient avoir une incidence directe sur la sécurité nationale, il devra en être dûment tenu compte». En outre, la déclaration 21 reconnaît que «règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière [...] pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines».

[87] Voir la section 7, partie A, ci-dessous.

[88] Ce paragraphe est manifestement un résumé très bref des principaux changements effectués dans les traités, pertinents dans le présent contexte.

[89] La période de transition prendra fin le 1er décembre 2014 (voir article 10 du protocole nº 36 sur les dispositions transitoires, annexé au traité de Lisbonne).

Cela signifiait également que la législation sur la protection des données qui relevait auparavant du troisième pilier et avait été adoptée par le Conseil à lui seul - parfois même juste avant l'entrée en vigueur du traité de Lisbonne[90] - devrait être remplacée par des règles adoptées par le Parlement et le Conseil en codécision pour être conforme à l'article 16, paragraphe 2, du TFUE. Cet élément est venu s'ajouter au contexte dynamique de la révision en cours du cadre juridique de l'Union européenne pour la protection des données.

D. Jurisprudence pertinente

En attendant, la charte joue un rôle de plus en plus important dans la jurisprudence de la Cour de justice. S'agissant de la portée de la charte, la Cour a jugé qu'elle s'appliquait chaque fois que les États membres agissent dans le cadre du droit de l'Union.[91] Le cas échéant, la législation nationale doit respecter le niveau de protection prévu par la charte, ainsi que la primauté, l'unité et l'effectivité du droit de l'Union concerné[92], ce qui peut même impliquer qu'une disposition constitutionnelle à l'échelle nationale ne sera plus applicable.[93] Cela signifie toutefois également que la charte s'appliquera pleinement dans le champ d'application de la législation de l'UE en matière de protection des données, aussi bien pour le législateur lui-même qu'a posteriori.

En ce qui concerne l'exigence d'«indépendance complète» d'une autorité de contrôle, le premier jugement en la matière a été rendu quelques mois après l'entrée en vigueur du traité de Lisbonne, sans que la Cour ne fasse référence à la charte.[94] Néanmoins, dans trois affaires ultérieures, elle a souligné que l'exigence de contrôle indépendant constituait un «élément essentiel» de la protection des données à caractère personnel résultant de l'article 8, paragraphe 3, de la charte et de l'article 16, paragraphe 2, du TFUE.[95] Il doit dès lors être présumé que la Cour s'est désormais également prononcée sur la signification de ces dispositions de droit primaire.

Récemment, la Cour a statué à deux reprises que les dispositions de la législation de l'Union étaient nulles en raison d'une atteinte injustifiée aux articles 7 et 8 de la charte. En novembre 2010, c'était le cas des dispositions sur la publication d'informations concernant les bénéficiaires d'aides agricoles sur un site web.[96] En avril 2014, il s'agissait de la conservation obligatoire de données de communication aux fins de l'application de la loi dans

[90] Voir, par exemple, les décisions du Conseil citées aux notes de bas de page 69 et 70.
[91] Arrêt du 26 février 2013, *Åkerberg Fransson*, C-617/10, points 17 à 21, non encore publié au Recueil
[92] Arrêt du 26 février 2013, *Melloni*, C-399/11, points 59 et 60, non encore publié au Recueil., et arrêt *Åkerberg Fransson*, point 29.
[93] Arrêt *Melloni*, point 64.
[94] Arrêt *Commission/Allemagne*, cité à la note de bas de page 51.
[95] Arrêt *Commission/Autriche*, points 36 et 37, et arrêt *Commission/Hongrie*, points 47 et 48 (tous deux cités à la note de bas de page 52), ainsi que l'arrêt *Digital Rights Ireland*, cité à la note de bas de page 97, point 68.
[96] Arrêt rendu dans les affaires jointes *Volker und Markus Schecke GbR et Hartmut Eifert*, C-92/09 et C-93/09, Rec. 2010, p. I-11063.

le cadre de la directive 2006/24/CE.[97] Dans une troisième affaire, en octobre 2013, la Cour a cependant jugé qu'une obligation de fournir les empreintes digitales en vue de leur stockage dans un passeport était valable.[98] Tous ces jugements ont été rendus à la suite de demandes de décisions préjudicielles émanant de juridictions nationales sur la validité de la législation européenne.

Bien que leur issue soit ferme et convaincante, ces trois affaires illustrent également une nette tendance de la Cour à effectuer une «lecture combinée» des articles 7 et 8 de la charte. Cette approche ne tient cependant pas compte de la nature essentiellement différente de ces deux dispositions et risque donc d'empêcher l'article 8 de produire tous ses effets.[99]

La première de ces trois affaires a été initiée par des agriculteurs allemands qui s'opposaient à la publication de leurs coordonnées et du montant des aides annuelles dont ils bénéficiaient. La juridiction de renvoi estimait que l'obligation de publier ces données sur un site web constituait une atteinte injustifiée au droit fondamental à la protection des données à caractère personnel, qui, selon elle, était essentiellement couvert par l'article 8 de la CEDH.[100]

La Cour de justice a relevé que, dans la mesure où le traité de Lisbonne était entré en vigueur, la validité de l'obligation devait être évaluée à la lumière de la charte.[101] Elle a également observé que le droit à la protection des données à caractère personnel, tel qu'énoncé à l'article 8 de la charte, était étroitement lié au droit au respect de la vie privée consacré à l'article 7 de cette même charte, mais n'était pas une prérogative absolue. C'est ce qu'il résulte de l'article 8, paragraphe 2, de la charte, qui autorise le traitement des données à caractère personnel si certaines conditions sont réunies, et de l'article 52, paragraphe 1, de la charte, qui admet que des limitations peuvent être apportées à l'exercice de droits tels que ceux consacrés aux articles 7 et 8 de celle-ci, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et libertés et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui. Elle a également observé que ces limitations correspondaient à celles tolérées dans le cadre de l'article 8 de la CEDH.[102]

La Cour a ensuite entrepris d'examiner si les dispositions de la législation européenne en cause violaient les droits garantis par les articles 7 et 8 de la charte et, le cas échéant, de

[97] Arrêt du 8 avril 2014 dans les affaires jointes *Digital Rights Ireland et Seitlinger*, C-293/12 et C-594/12, non encore publié au Recueil.
[98] Arrêt du 17 octobre 2013, *Michael Schwarz/Stadt Bochum*, C-291/12, non encore publié au Recueil. Contrairement aux arrêts *Schecke* et *Digital Rights Ireland*, cet arrêt n'a pas été rendu par la grande chambre.
[99] Pour une analyse critique, voir également Kranenborg, H., «Commentary on Article 8», dans Peers, S., *et al.* (eds.), *The EU Charter of Fundamental Rights: a Commentary*, 2014, 223, pages 229 à 231 et 260 à 262.
[100] Arrêt *Schecke*, points 30, 31 et 44.
[101] Arrêt *Schecke*, points 45 et 46.
[102] Arrêt *Schecke*, points 47 à 52.

déterminer si cette atteinte était justifiée au regard de l'article 52 de la charte. En ce qui concerne la première question, se fondant sur la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la CEDH et sur sa position dans l'affaire *Österreichischer Rundfunk*, la Cour a conclu que la publication sur un site web des données relatives aux montants précis constitue une ingérence dans leur vie privée au sens de l'article 7 de la charte.[103] Elle a également jugé que la publication constituait un traitement de données à caractère personnel relevant de l'article 8, paragraphe 2, de la charte et que les agriculteurs n'avaient pas consenti à la publication, si bien qu'il y avait également eu une ingérence dans le droit à la protection des données à caractère personnel au sens de l'article 8 de la charte.[104] En ce qui concerne la seconde question, la Cour a jugé en substance que l'ingérence n'était pas justifiée étant donné que rien ne démontrait que le législateur avait envisagé d'éventuelles autres solutions moins intrusives.[105]

Cette dernière conclusion a envoyé un message puissant sur la nécessité de preuves empiriques justifiant toute mesure intrusive. Cependant, la conclusion que la publication portait atteinte aux articles 7 et 8 de la charte ne semble pas tout à fait convaincante. En tout état de cause, l'absence de consentement était plus pertinente en ce qui concerne l'article 7 que l'article 8, et ce en dépit du fait que l'article 8, paragraphe 2, cite précisément le consentement comme *un exemple* de fondement légitime pour le traitement des données à caractère personnel. L'argument est qu'un consentement valable aurait très probablement empêché la Cour de conclure à une violation de l'article 7, alors que cette dernière n'a pas prêté attention à la seconde option énoncée à l'article 8, paragraphe 2, à savoir «un autre fondement légitime prévu par la loi». Elle aurait alors constaté que la réponse à la question de savoir si cette option s'appliquait ne pouvait dépendre que de son analyse de l'article 7 et non de l'article 8 en même temps. En effet, le fait que la publication constituait un traitement de données à caractère personnel relevant du champ d'application de l'article 8, paragraphe 2, n'en faisait pas une violation de l'article 8 en l'absence d'une seule des options de légitimité possibles. Néanmoins, il est clair que le fait même que la publication était une ingérence injustifiée dans le droit consacré à l'article 7 démontrait également qu'elle ne répondait pas aux exigences de l'article 8, paragraphe 2, et c'est peut-être ce que la Cour aurait dû dire.

L'approche de la Cour est encore plus explicite et radicale dans le deuxième arrêt cité ci-dessus concernant le stockage d'empreintes digitales dans un passeport. En l'espèce, un ressortissant allemand avait refusé que l'on relève ses empreintes digitales et contestait la validité des dispositions applicables en invoquant une violation des droits consacrés aux articles 7 et 8 de la charte.[106]

[103] Arrêt *Schecke*, points 56 à 59.
[104] Arrêt *Schecke*, points 60 à 64.
[105] Arrêt *Schecke*, points 81 à 86.
[106] Arrêt *Schwarz*, point 12.

En réponse, la Cour a débuté par «lecture conjointe» des articles en question, tout en affirmant qu'en règle générale, tout traitement des données à caractère personnel par un tiers était susceptible de constituer une atteinte auxdits droits.[107] Ce point de départ semble confondre la vaste portée de l'article 8 - qui couvre en principe tout traitement de données à caractère personnel - et la question de fond consistant à savoir quand il y a atteinte à l'article 7 ou à l'article 8. De surcroît, partant du fait que le prélèvement des empreintes digitales d'une personne et leur conservation dans un passeport peuvent être considérés comme un traitement de données à caractère personnel, la Cour conclut ensuite que le prélèvement d'empreintes digitales et leur stockage sur la base des dispositions applicables constitue une atteinte au droit au respect de la vie privée et au droit à la protection des données à caractère personnel.[108]

Dans son examen de la justification de «cette double atteinte», la Cour relève premièrement que les citoyens ne peuvent s'opposer librement au traitement de leurs empreintes digitales et que les demandeurs de passeports ne sauraient donc être considérés comme ayant consenti à un tel traitement.[109] La Cour examine ensuite si le traitement des empreintes digitales peut se justifier «en vertu d'un autre fondement légitime prévu par la loi». Après une analyse sur le fond à la lumière de l'article 52, paragraphe 1, de la charte, la Cour conclut que c'est en effet le cas des dispositions en cause en ce qui concerne les articles 7 et 8 de la charte.[110]

Il est frappant de voir à quel point cette analyse était totalement axée sur le traitement des données à caractère personnel et les conditions prévues à l'article 8 et à l'article 52, paragraphe 1, de la charte. Une autre approche plus convaincante aurait consisté en ce que la Cour - dans le droit fil de la jurisprudence de la Cour européenne des droits de l'homme[111] - conclue que le prélèvement d'empreintes digitales et leur stockage constituaient une ingérence dans le droit au respect de la vie privée consacré à l'article 7, mais étaient justifiés selon les critères établis à l'article 52, paragraphe 1. Or, la Cour a apparemment constaté une ingérence dans le droit consacré à l'article 8 avant de vérifier s'il existait «un autre fondement légitime prévu par la loi». De façon paradoxale, la conclusion que les dispositions en cause étaient effectivement valables ne fait que confirmer que l'établissement d'une violation de l'article 8 était prématuré.

Dans la troisième affaire mentionnée ci-dessus, qui concernait la conservation obligatoire de données de communication aux fins de l'application de la loi, il a été demandé à la Cour

[107] Arrêt *Schwarz*, points 23 à 25.
[108] Arrêt *Schwarz*, points 26 à 30.
[109] Arrêt *Schwarz*, point 32.
[110] Arrêt *Schwarz*, points 33, 34 et 63.
[111] Voir, par exemple, Cour européenne des droits de l'homme, *S et Marper/Royaume-Uni*, requêtes nº 30562/04 et nº 30566/04, CEDH 2008-V, points 78 à 86.

d'examiner la validité de la directive sur la conservation des données[112] à la lumière des articles 7 et 8 de la charte. En l'espèce, la Cour s'est concentrée bien davantage sur l'article 7 - le droit au respect de la vie privée - et a jugé que l'ingérence dans ce droit avait été «d'une vaste ampleur» et «particulièrement grave», et qu'elle ne pouvait être justifiée.[113] Cependant, elle a également mentionné à cet égard l'article 8 sur le droit à la protection des données à caractère personnel.

Dans ses remarques liminaires, la Cour commence par relever qu'«une telle conservation des données relève également de l'article 8 de [la charte] en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article».[114] La Cour constate ensuite que «si les renvois préjudiciels dans les présentes affaires soulèvent notamment la question de principe de savoir si les données des abonnés et des utilisateurs inscrits peuvent ou non, au regard de l'article 7 de la charte, être conservées, ils concernent également celle de savoir si la directive 2006/24 répond aux exigences de protection des données à caractère personnel découlant de l'article 8 de la charte».[115] Ces deux affirmations reflètent correctement une vision particulière du rôle de l'article 8: il est vu comme une source d'*exigences* pour le traitement des données à caractère personnel relevant de son champ d'application. Cependant, quelques points plus tard, la Cour observe soudainement: «De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la charte puisqu'elle prévoit un traitement des données à caractère personnel».[116]

Cette dernière observation n'est pas compatible avec les deux affirmations précédentes et avec la nature différente des articles 7 et 8. Une fois encore, la Cour conclut qu'il y a eu atteinte à l'article 8 avant de vérifier s'il a été satisfait aux «exigences de protection des données découlant de cet article». En effet, l'article 8 autorise le traitement des données à caractère personnel tant que ses exigences sont satisfaites. En l'espèce, la réponse aurait été que le «fondement légitime prévu par la loi» manquait, mais il n'était possible d'arriver à cette conclusion qu'au terme d'un examen de l'éventuelle justification de l'ingérence. En tout état de cause, la décision de la Cour précise très clairement qu'une telle justification faisait défaut.

Dès lors, les trois affaires montrent que la Cour semble toujours aux prises avec le véritable rôle de l'article 8 de la charte. Dans les affaires ayant trait à l'indépendance des autorités de

[112] 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, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54.
[113] Arrêt *Digital Rights Ireland*, points 37 et 70
[114] Arrêt *Digital Rights Ireland*, point 29.
[115] Arrêt *Digital Rights Ireland*, point 30.
[116] Arrêt *Digital Rights Ireland*, point 36.

contrôle, ce rôle était manifeste: il manquait un «élément essentiel» de la protection des données à caractère personnel prévu à l'article 8, paragraphe 3.[117] De même, il pourrait y avoir une atteinte à l'article 8 s'il n'était pas satisfait à un ou plusieurs des autres éléments essentiels énoncés dans cet article - comme le traitement loyal, la limitation des finalités, les droits d'accès et de rectification. Quant à savoir si une telle limitation du droit est justifiée ou non, la réponse dépendra ensuite d'une évaluation à la lumière de l'article 52.

5. La révision de la directive 95/46/CE

A. Origine de la révision

L'article 33 de la directive 95/46/CE exige de la Commission qu'elle fasse périodiquement un rapport sur l'application de la directive et qu'elle l'assortisse, le cas échéant, des propositions de modification appropriées.

Le premier rapport a été publié en mai 2003, après un processus de révision approfondi et ouvert.[118] Ce rapport a mis en évidence une série de problèmes, parmi lesquels des divergences considérables entre les États membres, soit en raison d'une mise en œuvre incorrecte, soit en raison de choix stratégiques différents à l'intérieur des marges de manœuvre laissées par la directive. Cependant, étant donné que l'expérience pratique de la directive était limitée, la Commission a estimé qu'il était trop tôt pour la modifier. Elle a préféré mettre en place un programme de travail visant à améliorer la mise en œuvre, attribuant des tâches différentes à elle-même, aux États membres, aux autorités de contrôle ainsi qu'aux autres parties intéressées. Le rapport invitait également le groupe de travail «Article 29» à encourager une meilleure mise en œuvre et à mener des investigations collectives dans les secteurs concernés.

Dans un second rapport, sur le suivi du programme de travail[119], publié en mars 2007, la Commission a indiqué que certains des problèmes mis en évidence existaient encore, mais qu'ils ne constituaient pas un réel problème pour le marché intérieur. Comme les solutions juridiques prévues par la directive étaient toujours appropriées et pouvaient également s'appliquer aux nouvelles technologies, la Commission a de nouveau estimé qu'il était trop tôt pour y apporter des modifications et a encouragé tous les acteurs à poursuivre leurs efforts

[117] Voir les références aux notes de bas de page 94 et 95. Cependant, ces arrêts ne font pas explicitement mention de l'«ingérence» dans l'article 8, paragraphe 3, de la charte.

[118] Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), 15.5.2003, COM(2003)0265 final. Voir également l'annexe technique, source de nombreuses informations (en anglais uniquement): «Analysis and impact study on the implementation of Directive EC 95/46 in Member States». Les deux documents sont disponibles à l'adresse suivante: http://ec.europa.eu/justice/data-protection/document/transposition/index_en.htm (dernière consultation le 31 mai 2014).

[119] Communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, 7.3.2007, COM (2007) 87 final, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/law/follow-up-work-programme/index_en.htm (dernière consultation le 31 mai 2014).

dans le cadre du programme de travail. En juillet 2007, le contrôleur européen de la protection des données a convenu que ce n'était pas encore le bon moment pour modifier la directive, mais a également estimé que cette modification était inévitable et qu'elle devait être bien préparée.[120]

Peu après, et avec une certaine réticence, la Commission a entamé les travaux préparatoires. En mai 2009, elle a lancé une consultation publique sur la nécessité de modifier le cadre juridique de la protection des données.[121] Cette consultation a suscité un très grand nombre de réactions provenant d'un vaste éventail de parties intéressées, dont une contribution substantielle du groupe de travail «Article 29» sur l'avenir de la protection de la vie privée.[122] Cela a coïncidé avec l'entrée en vigueur du traité de Lisbonne en décembre 2009, qui a introduit une nouvelle base juridique horizontale en matière de protection des données, et avec la nomination d'une nouvelle Commission chargée d'un programme plus conséquent en matière de droits de l'homme.[123]

En novembre 2010, la Commission a publié l'esquisse d'une «approche globale de la protection des données à caractère personnel dans l'Union européenne», qu'elle entendait fonder sur cette nouvelle base juridique.[124] Cette approche consistait à «renforcer les droits des personnes», à «renforcer la dimension "marché intérieur"» et à «assurer un plus grand respect des règles de protection des données», et couvrait également la «dimension mondiale de la protection des données». Les propositions relatives à un nouveau cadre devaient être présentées en 2011.[125] Dans une deuxième étape, la Commission évaluerait la nécessité d'adapter d'autres instruments juridiques à ce nouveau cadre général, au sein duquel elle inclurait également le règlement (CE) n° 45/2001 applicable aux institutions et organes de l'Union européenne.[126] En janvier 2011, le contrôleur européen de la protection des données

[120] Avis du CEPD du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255 du 27.10.2007, p. 1

[121] Voir les informations disponibles (en anglais uniquement) à l'adresse suivante: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm (dernière consultation le 31 mai 2014).

[122] Groupe de travail «Article 29» sur la protection des données et groupe de travail «Police et justice», contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée le 1er décembre 2009 (WP 168), disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_fr.pdf

[123] Mme Viviane Reding, vice-présidente de la Commission, en charge de de la justice, des droits fondamentaux et de la citoyenneté, a fait de la réforme de la législation en matière de protection des données une de ses premières priorités.

[124] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions: «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», COM (2010) 609 final. Voir également, Reding, V., «The upcoming data protection reform for the European Union», *International Data Privacy Law*, 2011, Vol. 1, Nº 1, pages 3 à 5.

[125] COM(2010) 609 final, page 18.

[126] Ibid., pages 18 et 19.

a marqué son accord avec les principaux axes de la communication, mais a demandé une approche plus ambitieuse sur un certain nombre de points.[127]

B. Les principaux axes de la révision

En janvier 2012, à peine plus tard qu'annoncé, la Commission a présenté une série de propositions destinées à actualiser et moderniser l'actuel cadre juridique de l'Union.[128] Ces propositions ont depuis lors fait l'objet de discussions nourries, à l'intérieur comme à l'extérieur du Parlement européen et du Conseil, et la révision approche maintenant le stade final du processus décisionnel politique: les négociations entre le Parlement et le Conseil sur les premiers résultats tangibles.[129]

Avant d'examiner le sujet plus avant, il est utile de résumer brièvement les raisons pour laquelle la révision en cours a lieu. Il y en a essentiellement trois. La première est la nécessité évidente de mettre à jour le cadre actuel, et en particulier la directive 95/46/CE, qui en constitue la pierre angulaire. En l'occurrence, «mettre à jour» revient avant tout à faire en sorte que cette directive demeure *efficace* dans la pratique. Lorsque la directive a été adoptée, l'internet en était encore à ses balbutiements, alors qu'aujourd'hui, nous vivons dans un monde où le traitement des données est omniprésent, de sorte que nous avons également besoin de garanties plus solides offrant des résultats acceptables dans la pratique. Les défis que constituent les nouvelles technologies et la mondialisation nous incitent à faire preuve d'imagination pour proposer des innovations en vue d'une protection plus efficace.

La deuxième raison est que le cadre actuel a donné lieu à un certain degré d'harmonisation, mais aussi à une *diversité* et une *complexité* accrues, et ce uniquement parce qu'une directive - du fait de sa nature juridique - doit être transposée en droit interne et que nous sommes maintenant confrontés à 28 versions, parfois très différentes, des mêmes principes fondamentaux. Cette diversité est évidemment trop extrême et engendre non seulement des dépenses superflues, mais aussi une perte d'efficacité. Le premier rapport sur la mise en application de la directive recensait un certain nombre de disparités entre les législations

[127] Avis du contrôleur européen de la protection des données du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée - «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», JO C 181/01 du 22.6.2011, p. 1.

[128] Voir la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions: «Protection de la vie privée dans un monde en réseau - Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle», COM (2012) 9 final. Voir également: Reding, V., «The European data protection framework for the twenty-first century», *International Data Privacy Law*, 2012, Vol. 2, Nº 3, pages 119 à 129, et Kuner, C. «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law», Bloomberg BNA *Privacy and Security Law Report*, 11 PVLR 215, 2.6.2012, pages 1 à 15.

[129] En mars 2014, le Parlement européen a adopté ses positions sur la proposition de règlement et la proposition de directive en première lecture, à des majorités écrasantes. Les discussions au sein du Conseil ont moins progressé. Le Conseil suit une «approche générale partielle» sur différents sujets et devrait aboutir à une position générale d'ici la fin 2014. En juin 2014, il a adopté une «approche générale partielle» sur le champ d'application territorial et le chapitre V du règlement concernant le transfert des données à caractère personnel à des pays tiers ou des organisations internationales.

nationales concernant le champ d'application et les définitions, ainsi que dans les pratiques utilisées aux fins de l'application et de la mise en œuvre.[130] Les efforts visant à réduire ces écarts n'ont manifestement pas été suffisamment productifs. Parallèlement, la nécessité de règles plus harmonisées s'est accrue sous l'effet de l'évolution des technologies et de la mondialisation. En d'autres termes, nous devons accélérer l'harmonisation, renforcer le système juridique et le rendre plus efficace, mais aussi plus *cohérent*, ce qui devrait permettre de réduire la diversité et la complexité *stériles* qui règnent actuellement.

La troisième raison a trait au nouveau cadre institutionnel de l'UE. Comme nous l'avons vu, le traité de Lisbonne a fortement mis l'accent sur la protection des droits fondamentaux et, tout particulièrement, sur le droit à la protection des données. L'article 8 de la charte des droits fondamentaux prévoit un droit séparé à la protection des données à caractère personnel, tandis que l'article 16 du TFUE propose une nouvelle base juridique horizontale pour l'adoption de règles en matière de protection des données garantissant une protection complète dans *tous* les domaines d'action de l'UE, que ce soit le marché intérieur, l'application des lois ou pratiquement tous les autres composants du secteur public.[131]

La révision en cours vise donc à mettre en place une protection des données à caractère personnel renforcée, plus efficace, plus cohérente et plus *exhaustive*. Le qualificatif «exhaustif» a également été utilisé par la Commission dans sa stratégie de réforme, quoique dans un sens beaucoup plus général: elle envisageait une «approche» exhaustive à mettre en œuvre en différentes étapes.[132]

L'ensemble de propositions présenté par la Commission en janvier 2012 se compose de deux éléments principaux: une proposition de règlement général sur la protection des données visant à remplacer l'actuelle directive 95/46/CE pour le secteur privé et la majeure partie du secteur public des États membres, et une proposition de directive destinée à remplacer l'actuelle décision-cadre 2008/977/JAI du Conseil en ce qui concerne le domaine de l'application de la loi[133].

La proposition de règlement a été accueillie comme un «grand pas en avant»[134] vers une protection des données à caractère personnel plus efficace et plus cohérente dans l'UE, mais

[130] Voir en particulier l'annexe mentionnée à la note de bas de page 118.
[131] Voir la section 4, partie C, ci-dessus.
[132] Voir note de bas de page 124.
[133] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM (2012) 11 final, et
proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM (2012) 10 final.
[134] Communiqué de presse du CEPD, 25 janvier 2012, disponible à l'adresse suivante:

plusieurs aspects importants appelaient également quelques clarifications et améliorations. Ces points ont été développés dans l'avis détaillé du contrôleur européen de la protection des données de mars 2012.[135] La circonstance que le règlement proposé serait directement contraignant dans tous les États membres accroît d'autant plus l'importance de veiller à ce que ses dispositions soient suffisamment claires.

Toutefois, l'architecture même de cet ensemble de propositions - un règlement et une directive - met également en évidence leur manque d'exhaustivité. C'est en effet là que le bât blesse: le niveau de protection offert par la proposition de directive est bien inférieur à celui de la proposition de règlement.[136] Ce problème peut être analysé à différents niveaux: l'option d'un règlement couvrant également le domaine de l'application du droit pénal était apparemment aller un pont trop loin pour la plupart des États membres, même en y incluant les limitations et exceptions appropriées. La deuxième option d'une directive ayant la même matière que le règlement, mais sous réserve des limitations et exceptions nécessaires, et laissant davantage de marge à la mise en œuvre nationale, était davantage concevable. Néanmoins, ce n'est pas ce que la Commission a proposé. Il est possible d'analyser les disparités qui en découlent au cas par cas, mais l'échange d'informations entre des entités publiques et privées, par exemple les autorités chargées de l'application de la loi et les banques, les opérateurs de téléphonie, les voyagistes, etc. est en pleine expansion, et un déséquilibre et une incohérence auront de graves conséquences pratiques à plus grande échelle. Il convient également de noter que les domaines connexes, comme la fiscalité, les douanes et le contrôle aux frontières, relèvent déjà de la directive 95/46/CE et seraient donc couverts par le règlement proposé.

En ce qui concerne le règlement, il convient de garder quelques généralités à l'esprit. Tout d'abord, en dépit de son caractère novateur, le règlement se caractérise également par une forte *continuité*. Tous les concepts et principes fondamentaux auxquels nous sommes habitués continueront d'exister, sous réserve de quelques éclaircissements et de petits changements dans les détails. Par exemple, le texte insiste à présent davantage[137] sur la «minimisation des données», en somme «la nécessité de ne pas traiter plus de données que nécessaire» ou «la meilleure protection consiste à traiter le moins de données possible». De

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-02_EC_DP_Proposal_FR.pdf (dernière consultation le 31 mai 2014)

[135] Avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, disponible à l'adresse suivante:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf (dernière consultation le 31 mai 2014).
Voir également le résumé de l'avis au JO C 192 du 30.6.2012, p. 7, et le communiqué de presse disponible à l'adresse suivante:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-07_DPReform_package_FR.pdf (dernière consultation le 31 mai 2014).

[136] Voir l'avis du CEPD, cité à la note de bas de page 135, points 49 à 74.

[137] Article 5, point c).

même, la «protection des données dès la conception», autrement dit «la prise en considération de la vie privée dès le début» - est désormais reconnue explicitement comme un principe général.[138] En outre, le texte apporte des précisions opportunes relatives au consentement: *lorsque* le consentement est nécessaire, il doit être réel et explicite.[139]

L'innovation réelle consiste essentiellement en «une protection des données plus efficace dans la pratique». Comme nous le verrons, il s'agit d'insister fortement sur la mise en œuvre des principes et sur le respect des droits et des obligations, pour veiller à ce que la protection soit assurée lorsqu'elle est requise dans la pratique. Parallèlement, le règlement prévoit la simplification et la réduction des coûts. Un exemple typique est la suppression dans une vaste mesure de la notification préalable des traitements à une autorité de protection des données. Elle restera nécessaire dans les seules situations qui présentent des risques spécifiques.[140] La proposition de règlement prévoit également la création d'un «guichet unique» pour les entreprises qui possèdent des établissements dans différents États membres. Cela implique l'introduction d'une autorité chef de file chargée de la protection des données qui devra agir en étroite coopération avec les autres autorités compétentes concernées.[141]

Un règlement directement contraignant offrira également une harmonisation renforcée - en principe: une seule législation applicable - et une cohérence accrue dans tous les États membres. En soi, il se traduira par une importante simplification des procédures et par une réduction notable des coûts pour les entreprises qui exercent leurs activités dans différents États membres. Parallèlement, des questions politiques se poseront inévitablement, dans la mesure où cela se fera au détriment des perceptions et préférences nationales concernant la meilleure approche à suivre en matière de protection des données. À un niveau plus détaillé, des questions se posent aussi quant à la manière exacte dont le règlement s'articulera avec le droit national et quant au fonctionnement précis du guichet unique. Nous reviendrons sur ces questions plus tard.[142]

C. Règlement général sur la protection des données

Il est maintenant temps de regarder aux grandes lignes de la proposition de règlement général sur la protection des données. Dans la mesure où il s'agit d'un document volumineux et plutôt compliqué, il est utile de l'aborder selon différents angles et d'étudier son champ d'application, ses principaux éléments et, enfin, sa dimension internationale.

[138] Article 23 relatif aux principes de «protection des données dès la conception et de protection des données par défaut».
[139] Article 4, point 8, et article 7.
[140] Articles 33 et 34.
[141] Article 51, paragraphe 2.
[142] Voir la section 6, parties A et C, ci-dessous.

Portée générale

Le champ d'application matériel du règlement est très proche de celui de l'actuelle directive: il s'applique à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l'exception de quelques situations qui correspondent en substance à celles mentionnées dans la directive.[143] Cependant, ces exceptions couvrent également le traitement des données à caractère personnel par les institutions et organes de l'Union européenne. Bien qu'elle fût censée constituer une exception technique qui serait suivie par une proposition distincte à un stade ultérieur, cette exception a soulevé à juste titre la question de savoir pourquoi le niveau de l'Union européenne lui-même devait être laissé à une seconde phase.[144]

Quoi qu'il en soit, il convient de souligner que le règlement a une portée générale: il s'appliquera au secteur privé comme au secteur public.[145] Ceci est tout à fait en phase avec ce qui est prévu par la directive actuelle. La possibilité d'opérer une distinction systématique entre secteur public et secteur privé dans cette directive avait été explicitement examinée et rejetée.[146] Cette approche s'est avérée tout à fait réalisable dans la pratique, dans la mesure où certaines dispositions - en particulier sur le traitement licite, renvoyant à des «missions publiques» - concernent à l'évidence davantage les pouvoirs publics, tandis que d'autres - faisant référence à des contrats ou à des intérêts légitimes - sont plus pertinentes pour les acteurs privés.[147]

La Cour de justice a confirmé que la directive actuelle s'applique également au secteur public d'un État membre.[148] Elle a toutefois souligné que le droit national ne peut constituer un motif légitime justifiant le traitement que s'il respecte pleinement les droits fondamentaux.[149] Cette position est renforcée par le fait que désormais, l'article 8 de la charte reconnaît également explicitement le droit à la protection des données à caractère personnel, et que l'article 16 du TFUE offre une base juridique horizontale explicite pour l'adoption de règles sur la protection des données à caractère personnel, au niveau européen comme dans les États membres, lorsque ceux-ci agissent dans le champ d'application du droit de l'UE, indépendamment du fait qu'il s'agisse du secteur privé ou du secteur public.

---

[143] Article 2.

[144] Article 2, paragraphe 2, point b). Le Parlement et le Conseil ont tous deux menacé de supprimer cette exception, à moins que la Commission ne présente une proposition distincte parfaitement cohérente.

[145] L'article 2 et toutes les autres dispositions générales n'effectuent aucune distinction entre le secteur public et le secteur privé.

[146] La première proposition de la Commission sur la directive (voir note de bas de page 31) reposait sur une distinction systématique, mais elle a été ensuite remplacée par une proposition révisée revêtant une portée plus générale.

[147] Voir l'article 7, points b), e) et f), de la directive 95/46/CE.

[148] Arrêt *Österreichischer Rundfunk*, cité à la note de bas de page 53, point 47. Voir également l'arrêt rendu dans l'affaire *Huber*, C-524/06, Rec. 2008, p. I-09705 et l'arrêt *Rijkeboer*, cité à la note de bas de page 62.

[149] Arrêt *Österreichischer Rundfunk*, points 68 à 72.

Parallèlement, il est nécessaire de réaliser une analyse plus pointue de la relation entre le droit de l'Union européenne et le droit national sur la base de la proposition de règlement. Croire que le règlement remplacera purement et simplement l'intégralité de la législation nationale pertinente en la matière est une erreur. Cela dépendra également de la manière dont le règlement lui-même abordera cette relation. À cet égard, le droit national et le droit européen coexisteront et interagiront de manières différentes. À titre d'exemple, le règlement complétera le droit national qui respecte entièrement les droits fondamentaux.[150]

En outre, il convient également d'examiner très minutieusement si, et le cas échéant où et comment, le règlement doit accorder une plus grande place à la spécification de ses dispositions dans le droit national. Cependant, il ne serait pas utile d'envisager une séparation du règlement en deux instruments différents, l'un pour le secteur public, l'autre pour le secteur privé ou commercial. Au contraire, un tel changement aurait des conséquences désastreuses, à la fois pour l'efficacité et pour la cohérence du nouveau cadre, en particulier pour les services à l'intersection des deux secteurs ou chevauchant la ligne de séparation entre eux. Cette distinction aurait probablement des effets différents pour les différents États membres et risquerait donc de donner aisément lieu à de nouvelles disparités et de saper le marché intérieur dans les situations transfrontières.

S'agissant de la substance du règlement, celui-ci renforce le rôle des partenaires clés, à savoir les individus (personnes concernées), l'organisation responsable (responsable du traitement) et les autorités de contrôle. Cela crée trois différentes perspectives qui, ensemble, renforcent la protection des données.

Contrôle des utilisateurs

La première perspective peut également être perçue comme améliorant le contrôle des personnes concernées sur le traitement des données qui les concernent. Il est indubitable que garantir un contrôle effectif pour les personnes concernées constitue un *objectif* majeur de la législation sur la protection des données, même si ce n'est pas la même chose que de reconnaître le droit formel à l'autodétermination en matière d'informations. L'article 8, paragraphe 2, de la charte souligne également l'importance que revêt ce contrôle en renvoyant aux droits d'accès et de rectification.

Il convient de souligner que les droits actuels de la personne concernée ont tous été confirmés dans le règlement, mais aussi renforcés, voire étendus.[151] L'exigence de consentement libre, spécifique, informé et non ambigu a été clarifiée et légèrement renforcée par la condition qu'il doit également être «explicite». Il s'agit d'une réaction opportune à une pratique répandue sur l'internet qui consiste à obtenir le consentement dans des circonstances très

[150] Voir la section 6, partie A, ci-dessous.

[151] Voir notamment les articles 11 à 19, qui prévoient désormais également des règles uniformes à travers l'Union européenne.

ambiguës. Parallèlement, le règlement est suffisamment flexible pour se satisfaire d'une action affirmative claire.[152]

Le droit d'opposition est également renforcé: il ne requiert plus de la personne concernée qu'elle démontre des raisons impérieuses et légitimes pour s'opposer. Au contraire, il exige du responsable du traitement qu'il justifie la nécessité impérieuse du traitement.[153] En outre, les moyens mis en œuvre pour veiller au respect de ces droits dans la pratique sont également renforcés.[154] Par ailleurs, la transparence est davantage mise en exergue[155] et une disposition introduit non pas un recours collectif à l'américaine, mais une action en nom collectif, permettant aux organisations d'intervenir au nom de leurs membres ou de leurs groupes constitutifs.[156]

Le «droit à l'oubli» a également fait l'objet de nombreuses discussions, mais à y regarder de plus près, il s'agit fondamentalement de mettre davantage l'accent sur la suppression des données lorsqu'il n'existe pas «de bonne raison de les conserver»[157], ainsi qu'une obligation de mettre en œuvre tous les efforts raisonnables afin de contacter des tierces parties en vue d'annuler les effets de la publication des données sur l'internet.[158] De même, le droit à la «portabilité des données» est fondamentalement une spécification du droit actuel consistant à demander la communication de toute donnée à caractère personnel dans une forme intelligible, mais aussi, désormais, dans un format particulier.[159]

Responsabilité

L'accent est principalement placé sur la responsabilité réelle des organisations chargées de la gestion des données. La responsabilité n'est pas une notion qui n'intervient qu'*à la fin*, en cas de problème. Il s'agit au contraire d'une obligation proactive de développer une *gestion* correcte *des données* dans la pratique. Cette responsabilité est traduite dans des expressions telles que «prendre toutes les mesures qui s'imposent afin de veiller à la mise en œuvre» et «vérifier et démontrer» que ces mesures «sont toujours efficaces».[160]

Il s'agit là de l'une des principales évolutions de la législation sur la protection des données. La *charge de la preuve* incombe donc dans de nombreux cas à l'organisation responsable qui

[152] Article 4, point 8.
[153] Article 19.
[154] L'article 12 prévoit, par exemple, la mise en place d'une «infrastructure» adéquate: il exige du responsable du traitement qu'il établisse «de manière proactive» des procédures permettant à la personne concernée d'exercer ses droits.
[155] Voir l'article 11 sur les règles internes transparentes et facilement accessibles, et sur la transparence des informations et de la communication.
[156] Articles 73 à 76.
[157] Dans l'arrêt *Google Spain*, cité à la note de bas de page 45, aux points 73, 74, 88, 93, 94, 98 et 99, la Cour va dans le même sens.
[158] Article 17.
[159] Article 18.
[160] Article 22.

doit, en d'autres termes, prouver l'existence d'une base juridique adéquate pour le traitement, la réalité du consentement et l'efficacité continue des mesures.[161] Cette évolution explique également l'utilisation fréquente du terme «responsabilité» dans les discussions à ce sujet.[162]

Le règlement prévoit également un certain nombre d'exigences spécifiques, telles que la nécessité d'une analyse d'impact relative au respect de la vie privée, à l'établissement de documentation et à la désignation d'un délégué à la protection des données.[163] Selon de nombreux observateurs, certaines de ces dispositions, notamment en ce qui concerne la documentation, étaient excessivement détaillées et ont donc suscité de nombreuses discussions, au Parlement comme au Conseil. Il se peut que certaines exceptions prévues dans ces mêmes dispositions n'aient pas été pleinement justifiées, y compris celles visant les petites et moyennes entreprises. Un meilleur équilibre de cette partie de la proposition pourrait sans doute résoudre ces deux problèmes. À cet égard, il est essentiel que les dispositions générales des cadres actuel et futur soient évolutives par nature. Des spécifications inadéquates risquent d'entraîner des exceptions inutiles. Cette recherche du bon équilibre s'opère maintenant en vertu de «l'approche basée sur les risques».[164]

Une disposition générale sur la notification des violations de la sécurité est également prévue.[165] Le droit de l'Union européenne limite désormais cette notification aux seuls fournisseurs de télécommunications.[166] On pourrait y voir un mécanisme de responsabilisation «à la fin», qui renforce la gestion des données du «cycle de vie».

Contrôle et mise en application

Un troisième point majeur du règlement concerne la nécessité de rendre la surveillance et le contrôle de l'application plus efficaces. Les garanties prévues concernant l'indépendance complète des autorités de contrôle ont été renforcées conformément à la jurisprudence de la Cour.[167]

En outre, le règlement confère aux autorités de contrôle des pouvoirs d'exécution renforcés dans tous les États membres.[168] Les amendes administratives s'élevant à des millions d'euros, soit des montants s'inspirant de la concurrence, ont beaucoup attiré l'attention, mais le message est le suivant: «aux grands maux les grands remèdes». De cette manière, la

[161] Article 5, point f); article 7, paragraphe 1, et article 22, paragraphe 1.
[162] Voir l'avis n° 3/2010 du groupe de travail «Article 29» sur le principe de responsabilité, adopté le 13 juillet 2010 (WP 173). Pour plus d'informations sur la responsabilité et la conformité, voir la section 7, partie B, ci-dessous.
[163] Articles 22, paragraphe 2, 28, 33 et 35 à 37.
[164] Voir la section 6, partie B, ci-dessous.
[165] Article 31.
[166] Article 4, paragraphes 3 à 5, de la directive 2002/58/CE (voir note de bas de page 63), tel que révisée en 2009.
[167] Article 47.
[168] Articles 53 et 79.

«protection des données» figurera à un rang beaucoup plus élevé parmi les priorités à l'ordre du jour des conseils d'administration des entreprises, ce qui est fort louable.

En réalité, nous constatons déjà une pratique en rapide expansion de mise en application plus stricte des lois, au moyen de différents outils à l'échelle nationale: sanctions correctives, amendes administratives, mais également quelques responsabilités renforcées. Cette tendance se poursuivra sans nul doute dans un avenir proche, renforcée si possible sur la base du règlement.

La coopération internationale entre les autorités de protection des données est également vivement encouragée et facilitée par le règlement.[169] L'instauration d'une autorité chef de file pour les entreprises possédant plusieurs établissements est accueillie positivement, même si, là encore, ladite autorité n'agira pas seule mais au sein d'un réseau, en étroite collaboration avec d'autres autorités compétentes.[170]

Un autre élément supplémentaire très important est l'instauration d'un mécanisme de contrôle de la cohérence dans le cadre du comité européen de la protection des données, qui sera construite sur la base de l'actuel groupe de travail «Article 29». Ce mécanisme vise à garantir la cohérence des résultats de la surveillance et de l'application à travers l'ensemble des États membres.[171]

Protection mondiale de la vie privée

Enfin, un dernier élément doit être relevé: la dimension internationale du règlement dans un sens plus large. Le champ d'application du nouveau cadre juridique a été clarifié et étendu. Les dispositions s'appliqueront non seulement à tous les traitements dans le cadre d'un établissement du responsable au sein de l'Union européenne[172], mais aussi aux livraisons de biens et prestations de services sur le marché européen à partir d'un établissement situé dans un pays tiers, ou aux modalités de contrôle du comportement des personnes concernées au sein de l'Union.[173]

Il s'agit d'une réalité de plus en plus présente dans le monde actuel de l'internet. Mais cette approche est également réaliste et s'appuie sur une réflexion commune en matière de protection des données dans de nombreux pays concernés aux quatre coins du globe.[174] La directive 95/46/CE a exercé une influence majeure sur les normes mondiales et il n'y a aucune raison de penser que ce sera différent pour le règlement. La puissance de marché

[169] Articles 45, 55 et 56.
[170] Articles 51, paragraphe 2. Voir également la section 6, partie C, ci-dessous.
[171] Articles 57 à 61, et 64 à 72.
[172] Comme expliqué récemment dans l'arrêt *Google Spain*, cité à la note de bas de page 45.
[173] Article 3.
[174] Voir la section 6, partie D, ci-dessous.

cumulée de 500 millions de consommateurs au sein de l'Union européenne contribuera également à garantir la conformité.

À cet égard, il convient d'ajouter que les autorités de protection des données développent une coopération internationale à plus grande échelle - par exemple, entre la Commission fédérale du commerce (Federal Trade Commission) aux États-Unis et les autorités de contrôle dans l'UE – au sein d'un réseau mondial d'autorités chargées du respect de la vie privée (GPEN).[175] Grâce à ce réseau, il sera possible de collaborer plus efficacement avec les acteurs mondiaux sur l'internet. Cette avancée bénéficie d'une convergence croissante des principes et pratiques de protection des données à travers le monde, également encouragée par les cadres du Conseil de l'Europe et de l'OCDE qui se chevauchent partiellement. [176]

Enfin, il convient de souligner que les dispositions sur les flux de données transfrontières de l'actuelle directive ont été plus amplement élaborées et, lorsque c'était possible, simplifiées. Une disposition spécifique relative aux règles d'entreprise contraignantes a été introduite et prévoit également plusieurs simplifications.[177]

6. Points clés du débat législatif

A. Un seul ensemble de règles applicables?

À la section 5, partie B, nous avons indiqué qu'un règlement offrira une harmonisation plus large - en principe: une seule législation applicable - et une plus grande cohérence dans tous les États membres. C'est sans aucun doute une réalisation importante. Dans le système actuel, le droit national d'un État membre s'applique généralement au traitement de données à caractère personnel effectué «dans le cadre des activités d'un établissement» du responsable du traitement sur le territoire dudit État membre.[178] Par conséquent, n'importe quel État membre risque d'être confronté à différentes législations nationales sur son territoire, en fonction du contexte dans lequel le traitement des données à caractère personnel est effectué. Il se peut par ailleurs que les personnes concernées soient confrontées à d'autres législations nationales que les leurs. À l'avenir, en principe, le règlement déterminera non seulement le champ d'application externe du droit de l'UE, mais aussi le droit applicable n'importe où au sein de l'Union.

Cela signifie-t-il pour autant qu'il n'existera qu'un seul ensemble de règles applicables? La Commission s'est servie de ce message à plusieurs reprises afin de glaner du soutien en

[175] Global Privacy Enforcement Network (https://www.privacyenforcement.net), créé par suite de la recommandation de l'OCDE du 12 juin 2007, relative à la coopération transfrontière dans l'application des législations protégeant la vie privée, disponible à l'adresse suivante: http://www.oecd.org/fr/internet/ieconomie/38876531.pdf (dernière consultation le 31 mai 2014).
[176] Voir la section 6, partie D, ci-dessous.
[177] Articles 40 à 45 (voir article 43 sur les règles d'entreprise contraignantes).
[178] Article 4, paragraphe 1, point a). Voir également note de bas de page 45.

faveur du règlement, et c'était également un argument important pour que le Parlement et les autres parties intéressées offrent leur appui. Cependant, cette assertion ne semble pas tout à fait justifiée, et ce au moins pour deux raisons.

La première est que le règlement est peut-être un élément important d'une approche globale, mais en aucun cas la seule. En fait, il semble faire partie d'une approche globale en différentes étapes, mais ni à court ou moyen terme ni à long terme, il n'est certain que le règlement fournira le seul ensemble de règles applicables à un quelconque sujet pertinent de la protection des données.[179] En revanche, il est plus vraisemblable que d'autres règles, peut-être plus spécifiques - comme l'actuelle directive 2002/58/CE sur la protection de la vie privée et les communications électroniques -, s'appliqueront également. Il serait bon que ces règles soient parfaitement cohérentes avec les exigences du règlement.

La seconde raison est plus fondamentale. Comme cela a été mentionné à la section 5, partie C, croire que le règlement remplacera purement et simplement la législation nationale en la matière est une erreur. Cela dépend également de la manière dont le règlement aborde la relation entre le droit de l'Union européenne et le droit national. À cet égard, le droit national et le droit européen coexisteront et interagiront d'au moins quatre manières différentes. Il se peut que le règlement *complète* la législation nationale ou, à l'inverse, qu'il autorise ou ordonne que la législation nationale complète le règlement et le *mette en application*. Dans plusieurs dispositions, le règlement autorise également, voire demande, que le droit national *spécifie* ou élabore ses règles dans certains domaines ou même que le droit national *s'écarte* des dispositions du règlement sous certaines conditions.[180]

Les dispositions relatives aux fondements d'un traitement licite contiennent des exemples qui illustrent la première catégorie (*complément* du droit national). Conformément à l'article 6, paragraphe 1, du règlement, le traitement des données à caractère personnel n'est licite que si et dans la mesure où il est, c), nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou e), nécessaire à l'exécution d'une mission effectuée dans l'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans les deux cas, le règlement complète les motifs de traitement qui, dans la plupart des cas, sont pour l'essentiel prévus en droit national.

Dans les deux autres catégories - *spécification* ou *distanciation* -, le règlement confère différents degrés de flexibilité à l'adoption de règles nationales sur certains sujets.[181] Dans certaines situations, cette souplesse est considérable, ce qui signifie qu'un grand espace est laissé à la diversité mais aussi aux règles applicables divergentes dans ces domaines. Il est

[179] Voir note de bas de page 124.
[180] Voir l'avis du CEPD du 7 mars 2012, cité à la note de bas de page 135, points 50 à 55. Les articles 46 à 49 requièrent des États membres qu'ils établissent une ou plusieurs autorités de contrôle indépendantes conformément à ces dispositions. Des exemples des trois autres catégories suivent immédiatement ci-après.
[181] Voir notamment l'article 21 (limitations) et les articles 80 à 85 (situations particulières).

probable que ce soit simplement la démonstration des limites de l'harmonisation et de la cohérence dans un contexte européen.

La plupart des États membres comptent un certain nombre de lois nationales qui peuvent ne pas traiter explicitement de la protection des données, mais qui contiennent néanmoins toute une série de dispositions sur la collecte, le stockage, l'échange ou la publication de données à caractère personnel, ou sur la manière dont les droits de la personne concernée doivent être exercés ou respectés dans un domaine particulier. Nombre de ces lois relèvent sans doute du champ d'application de la directive 95/46/CE et peuvent avoir été adoptées dans le cadre de sa mise en application en droit interne.[182] Dans la plupart des États membres, ces lois seront cohérentes avec la législation nationale en matière de protection des données. Elles seront plus fréquentes dans le secteur public, mais peuvent également concerner d'autres secteurs,

Il est évident que ces lois devront être modifiées si elles ne sont pas compatibles avec le règlement dans sa version finale, si leurs dispositions n'offrent pas un fondement au traitement licite des données à caractère personnel (comme dans la première catégorie) et ne sont pas prévues de quelque manière que ce soit par le règlement. Ainsi, ces lois nationales devront être alignées sur les dispositions réglementaires, y compris le principe général de libre circulation des données à caractère personnel au sein de l'Union, tel qu'exprimé désormais à l'article premier dudit règlement.

Cette brève analyse démontre qu'il n'y aura pas un ensemble unique de règles applicables et que la mise en place de la relation précise entre le droit de l'Union et le droit national nécessitera un examen minutieux et des mises au point, à la fois au niveau de l'Union et au niveau national, surtout si le règlement continue de s'appliquer au secteur privé et au secteur public. D'autre part, le règlement aura accompli un pas en avant énorme et souhaitable en offrant une harmonisation plus large et une plus grande cohérence si ces efforts sont fructueux.

B. Charges administratives et innovation

Certes, la proposition de règlement a été saluée, mais elle a également suscité de vives critiques de la part des organisations professionnelles et fait l'objet de campagnes de lobbying sans précédent. En un sens, cela ne fait que confirmer l'importance de cette question pour nos économies numériques et pour nos sociétés de plus en plus dépendantes des TIC dans leur ensemble. Ces critiques font ressortir deux préoccupations prédominantes qui se chevauchent en partie: d'une part, que le règlement engendrera de lourdes charges administratives pour les responsables du traitement des données, tout particulièrement dans les petites et moyennes entreprises, et d'autre part, qu'il étouffera l'innovation dans les domaines cruciaux pour le développement de nos économies.

[182] Comme la sécurité sociale, la fiscalité, les registres de la population, l'État civil, etc. Voir également les arrêts de la Cour cités à la note de bas de page 148.

Les deux sujets sont remarquables car la Commission a été très soucieuse de mettre en évidence que la proposition de règlement prévoit également une simplification et une réduction des coûts. À la section 5, partie B, nous avons donné trois exemples: la nette réduction de l'obligation de notification préalable des autorités de protection des données, l'introduction d'un guichet unique pour les entreprises ayant des établissements dans plusieurs États membres, et le fait qu'un règlement directement contraignant assure une harmonisation plus large et une cohérence accrue dans l'ensemble des États membres. Il convient également de souligner que le respect de la vie privée et la confiance sont des thèmes clés de la stratégie numérique de la Commission, un volet essentiel de la stratégie UE 2020 pour une Europe intelligente, durable et inclusive.[183] Des garanties solides et efficaces en faveur de la protection des données à caractère personnel visent en effet également à contribuer à la croissance économique et la création d'emplois. Ce débat semble donc présenter les deux aspects d'une même question et s'insère bien dans la recherche du juste équilibre entre les moyens et les finalités, et entre les coûts et les avantages. La nécessité de proportionnalité est un principe plus général du droit de l'Union européenne qui revêt tout autant d'importance.[184]

Il convient de formuler trois observations à cet égard. Premièrement, personne n'aimerait voir l'innovation étouffée, mais en même temps, il serait stupide de détourner le regard du fait que l'innovation peut avoir des côtés négatifs que les décideurs publics doivent aborder. Cela vaut tout particulièrement pour l'essor des technologies de l'information qui sont devenues aujourd'hui omniprésentes dans nos sociétés. Le concept de protection des données a été élaboré afin de fournir une protection juridique aux personnes contre l'utilisation inappropriée ou excessive des technologies de l'information aux fins du traitement de données les concernant. Le droit à la protection des données à caractère personnel est désormais devenu un droit fondamental et s'est vu renforcé par une base juridique impérative destinée à garantir son efficacité continue au sein d'une société moderne. Cependant, le contenu de ces règles doit toujours être en accord avec l'objectif poursuivi et ne pas sortir de ce cadre. En même temps, il convient d'encourager davantage l'innovation à tenir compte des exigences de la protection des données d'emblée («respect de la vie privée dès la conception»), ce qui est moins cher et plus efficace que la mise en conformité rétroactive des technologies.

Deuxièmement, il est indispensable d'opérer une distinction nette entre les mesures visant à garantir le respect des règles existantes et les nouvelles exigences légales. Il se peut que les organisations qui ont jusqu'à présent sous-estimé, voire ignoré, l'importance des règles

[183] Voir http://ec.europa.eu/digital-agenda (en anglais uniquement) et http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_fr.htm (dernière consultation le 31 mai 2014).
[184] Voir l'article 5 du TUE, et le protocole nº 2 sur l'application des principes de subsidiarité et de proportionnalité joint aux traités.

existantes en matière de protection des données pour leurs activités particulières[185] - en ligne ou hors ligne - et se trouvent par conséquent dans une situation de non-conformité avec le droit applicable, soient désagréablement surprises par les efforts visant à donner plus d'effectivité et d'efficacité aux principes qui existent depuis un certain temps. Une partie du lobbying intensif mené contre la proposition de règlement suggère que c'est en effet le cas pour les nouveaux arrivants et peut-être aussi pour certains opérateurs à succès sur l'internet. Cependant, ce n'est pas une raison pour négliger l'objectif légitime que vise l'offre de meilleures garanties afin d'assurer l'effectivité permanente d'un droit fondamental.

En troisième lieu, ce qu'il reste donc, c'est la recherche du juste équilibre entre la nécessité d'assurer la protection efficace des personnes dans un environnement souvent dynamique et la nécessité d'éviter des charges administratives inutiles. La discussion à ce sujet a été dans une grande mesure déclenchée par le fait que les dispositions en cause de la proposition de règlement ne mettaient pas assez l'accent sur les principes généraux de responsabilité et de transparence des responsables du traitement des données, mais en revanche allaient trop loin dans les exigences spécifiques, qui à leur tour conduisaient à un certain nombre d'exceptions particulières, entre autres pour préserver les petites et moyennes entreprises de charges administratives excessives.[186] Il est vrai que certains détails étaient inévitables pour assurer une application cohérente du règlement à travers l'Union européenne, mais mettre davantage l'accent sur les principes généraux de responsabilité aurait procuré un meilleur cadre pour l'analyse. Une question pertinente est, par exemple, ce que comporte l'obligation générale pour le responsable du traitement d'adopter des «mesures appropriées» dans les situations où les exigences spécifiques ne s'appliquent pas.

Ce problème est maintenant abordé dans le cadre de «l'approche basée sur les risques». Cette approche doit être soigneusement distinguée de la notion de «risque» comme condition *minimale* pour l'application de toute protection, et encore davantage d'une approche selon laquelle la protection ne s'appliquerait qu'aux traitements présentant le plus de risques. En effet, il convient de tenir compte du fait que le risque est intrinsèque à tout traitement de données. Une approche «progressive» basée sur les risques suggérerait, au contraire, que des obligations plus détaillées devraient s'appliquer lorsque le risque est accru et des obligations moins fastidieuses lorsque le risque est moindre. Cette approche présente deux avantages considérables: tout d'abord, elle entend que les efforts de conformité devraient être avant tout dirigés vers les domaines où ils sont le plus nécessaires, eu égard par exemple à la sensibilité des données ou au risque que comporte un traitement donné, plutôt que de s'adonner à un exercice consistant à cocher des cases afin de satisfaire des exigences bureaucratiques. Ensuite, elle implique que les domaines présentant un risque minimal pourraient faire l'objet

[185] À cet égard, l'arrêt *Google Spain* (cité à la note de bas de page 45) peut avoir tiré la sonnette d'alarme pour les opérateurs, les incitant à repenser leurs modèles économiques actuels et les arrangements juridiques connexes.

[186] Voir les articles 22 à 37 et la section 5, partie C, ci-dessus.

d'une méthode plus légère. Il importe toutefois de souligner que les dispositions générales des cadres actuel et futur sont évolutives par nature et devraient dès lors être toujours respectées. Les droits particuliers de la personne concernée devraient également être toujours garantis, indépendamment du risque associé au traitement.

Des efforts sont actuellement déployés pour décrire plus amplement la notion de «risque», qui implique nécessairement un jugement. Dans l'intérêt de la sécurité juridique, le règlement devrait énoncer des critères suffisamment clairs à l'aune desquels l'évaluation des risques doit être réalisée par les responsables du traitement, comprenant à la fois des facteurs objectifs (comme le nombre de personnes concernées par un traitement donné) et des notions plus subjectives (comme les conséquences néfastes éventuelles pour la vie privée de la personne).[187] Sur la base de ces critères généraux exposés dans le règlement, d'autres orientations pourraient être formulées, soit par le comité européen de la protection des données, soit au moyen d'actes délégués, tous deux sous réserve d'un contrôle et d'une application appropriés. Une telle approche offrirait une plus grande sécurité juridique aux responsables du traitement, une protection plus efficace aux personnes et une souplesse suffisante pour résister à l'épreuve du temps.

C. Guichets uniques pour les citoyens et les entreprises

Une des nouveautés apportées par la proposition de règlement est la création d'un guichet unique pour les entreprises ayant des établissements dans plusieurs États membres.[188] Pour simplifier, lorsque le traitement des données à caractère personnel a lieu dans plus d'un État membre, une autorité de contrôle unique devrait assurer le suivi des activités du responsable du traitement ou du sous-traitant à travers l'Union européenne et prendre les décisions y afférentes. D'après la proposition, il s'agirait normalement de l'autorité de protection des données (ci-après la «DPA») nationale de l'État membre où l'«établissement principal» de l'entité responsable est situé, aussi appelée «autorité chef de file». Le rôle d'une autorité chef de file *ne* doit *pas* être perçu comme une compétence *exclusive*, mais comme une méthode de coopération structurée avec les autres autorités de contrôle compétentes à l'échelle locale. En effet, l'autorité chef de file sera largement tributaire de la contribution et du soutien des autres autorités de protection des données aux différents stades du processus.

[187] Un élément de risque complètement différent concerne les conséquences auxquelles les contrôleurs s'exposent personnellement en termes de sanctions, de responsabilité et de perte de confiance des consommateurs, en cas de non-respect.

[188] Voir notamment l'article 51, paragraphe 2. Voir aussi le point 2 de la lettre du CEPD du 14 février 2014 au Conseil, concernant les avancées réalisées sur le paquet de mesures pour une réforme de la protection des données, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-02-14_letter_Council_reform_package_FR.pdf (dernière consultation le 31 mai 2014).

La proposition de règlement était plutôt ambiguë sur ce point. La Commission semblait suggérer que le rôle de l'autorité chef de file était une compétence exclusive. Par ailleurs, le règlement ne dotait pas explicitement l'autorité chef de file de pouvoirs suffisants pour agir en dehors de sa propre juridiction. Parallèlement, il prévoyait un lien solide entre les dispositions sur la coopération mutuelle avec d'autres autorités de contrôle, ce qui devrait en effet permettre à l'autorité chef de file de jouer son rôle de manière efficace. De plus, toute décision de l'autorité chef de file ne serait exécutoire à travers l'Union européenne que si l'affaire avait été traitée dans le cadre d'un mécanisme de contrôle de la cohérence associant l'ensemble des autres autorités de contrôle nationales au sein du comité européen de la protection des données.[189] Ainsi, les autres autorités de contrôle (compétentes à l'échelle locale) seraient en mesure de participer à la coopération et d'influer sur l'issue de la décision finale de l'autorité chef de file dans toutes les affaires concernées.

Le principe de guichet unique est un élément important de l'harmonisation du cadre juridique de l'UE pour la protection des données. Il a été proposé par la Commission afin d'améliorer la cohérence de la mise en application, de garantir la sécurité juridique et de réduire les charges administratives excessives pour les responsables du traitement et les sous-traitants qui exercent leurs activités dans plusieurs États membres. Ce principe réduit également la fragmentation du paysage de la protection des données. Il importe que les entreprises puissent traiter (idéalement) avec un seul interlocuteur au lieu (éventuellement) de 28 régulateurs nationaux.

Après avoir approuvé ce principe en octobre 2013, le Conseil a néanmoins émis un certain nombre d'objections soulevées par son propre service juridique à l'encontre dudit principe.[190] Ces objections remettaient en cause sa compatibilité avec la charte des droits fondamentaux, en particulier son article 47, qui garantit le droit à un recours efficace devant un tribunal et le droit à un procès équitable, correspondant essentiellement à l'article 13 et à l'article 6, paragraphe 1, de la CEDH. La principale inquiétude semblait être la question de la «proximité» entre l'autorité de protection des données chef de file qui statue sur un cas particulier et le citoyen individuel, cette question étant perçue comme un aspect important de la protection des droits individuels. De manière plus générale, le principe de guichet unique était considéré comme profitable aux multinationales, au détriment des citoyens individuels.

Cette interprétation du principe de guichet unique dépeint un portrait excessivement négatif des propositions actuellement sur la table. En effet, il est possible de concilier ce principe avec une norme rigoureuse de protection des droits fondamentaux des citoyens, y compris

[189] Article 63.
[190] Voir la note de la présidence, du 26 mai 2014, au Conseil sur le mécanisme de guichet unique, disponible à l'adresse suivante: http://register.consilium.europa.eu/doc/srv?l=FR&f=ST%2010139%202014%20INIT (dernière consultation le 30 juin 2014).

ceux garantis par l'article 47 de la charte. Cette position se fonde sur un certain nombre de considérations.

Avant tout, il importe de souligner qu'à l'heure actuelle, conformément à l'article 28, paragraphe 6, de la directive 95/46/CE, l'autorité chargée de la protection des données a toujours compétence pour exercer les pouvoirs dont elle est investie, y compris celui d'instruction des plaintes, sur le territoire de l'État membre dont elle relève. Cependant, à moins que la plainte ne vise un responsable du traitement (ou un sous-traitant) ayant un établissement ou son équipement dans l'État membre en question, les pouvoirs effectifs de cette autorité pour appliquer la législation sur la protection des données peuvent s'avérer limités dans la pratique. La nécessité d'appliquer, dans un cas particulier, la législation nationale d'un autre État membre et l'absence de possibilité de mener une enquête ou d'imposer des sanctions en l'absence physique du responsable du traitement ou du sous-traitant peuvent cependant rendre le recours à l'autorité locale de protection des données purement théorique et en grande partie inefficace.

En revanche, la proposition de règlement vise à assurer un cadre juridique uniforme et à mettre en place plusieurs mécanismes garantissant une mise en application efficace dans la pratique. Les citoyens se verraient explicitement accorder le droit d'introduire une réclamation auprès de la DPA locale ou toute autre DPA afin d'exercer leurs droits.[191] Dans la pratique, la DPA locale fonctionnera probablement comme le guichet unique pour les citoyens au sein de la juridiction concernée. Cependant, dans les cas où à l'heure actuelle, une DPA disposerait d'options limitées, le nouveau règlement assurerait une application efficace par l'autorité de contrôle chef de file, dans le cadre du guichet unique pour les entreprises (avec l'appui d'un mécanisme de contrôle de la cohérence), et, au besoin, en associant la DPA locale compétente. En outre, les personnes affectées auront toujours la possibilité d'intenter une action juridique contre une entreprise établie dans leur pays devant les cours et tribunaux nationaux eu égard à une violation alléguée du règlement.[192]

De ce point de vue, le règlement aura une incidence très positive sur les possibilités qui s'offrent aux personnes de faire valoir leur droit à la protection des données, et apportera ainsi une amélioration significative pour les personnes concernées relativement à leur droit à un recours effectif, consacré par l'article 47 de la charte.

Le règlement prévoit également le réexamen juridictionnel des décisions prises par une DPA. Lorsque le principe de guichet unique s'applique, une personne qui souhaite contester une décision prise par l'autorité chef de file devrait le faire devant une juridiction de l'État

[191] Article 73.
[192] Article 75.

membre duquel relève l'autorité chef de file[193], ce qui se traduirait souvent, dans la pratique, par l'obligation d'intenter une action dans un autre État membre.

Dans ce contexte, la seule nécessité pour le citoyen de saisir les tribunaux d'un État membre autre que son pays de résidence ne le prive pas en soi d'une protection judiciaire effective. En vertu de l'actuelle directive 95/46/CE, il est également possible que les citoyens qui souhaitent former une réclamation à l'encontre du traitement de données à caractère personnel par une entreprise qui exerce ses activités dans de nombreux États membres doivent s'adresser eux-mêmes à une DPA particulière et, en cas de contestation des décisions adoptées par cette dernière, qu'ils doivent engager des poursuites dans ce même État membre. Jusqu'à présent, il n'y a eu aucune raison de remettre cette caractéristique de l'actuel système en question à la lumière de la charte.

Le principe de guichet unique proposé est également critiqué en ce qu'il crée des obstacles excessifs pour les citoyens qui souhaitent former un recours juridictionnel en raison de la distance géographique, de la méconnaissance d'un système juridique étranger, de la nécessité d'entamer et de mener un procédure dans une langue étrangère, ou des coûts qu'impliquent cette procédure.

L'alternative proposée à cet égard semble être la création d'un organe européen, doté de la personnalité juridique, qui jouerait le rôle de guichet unique, aussi bien pour les citoyens que pour les entreprises. Cette solution nécessiterait une centralisation fondamentale de l'actuelle structure décentralisée que présente le contrôle de la protection des données, sans nécessairement faciliter le processus décisionnel dans un délai raisonnable et, assurément, sans offrir une plus grande «proximité» aux citoyens et aux entreprises. Plus important encore, il n'apparaît pas indispensable de garantir une meilleure protection des droits fondamentaux des citoyens.

Il importe de garder à l'esprit le fait que, dans la plupart des cas, l'ensemble des acteurs concernés (personnes concernées, responsable du traitement et DPA) résideront toujours dans un seul pays. Par conséquent, le principe de guichet unique pour les entreprises ne trouverait à s'appliquer que dans un nombre relativement limité de situations. En outre, il pourrait être possible d'exclure les problèmes de nature majoritairement locale, comme ceux survenant dans le cadre de la législation nationale. En d'autres termes, bien que certains des cas restants puissent avoir une incidence nette, les cas où les citoyens sont affectés par les décisions d'une DPA chef de file située dans un État membre autre que leur propre pays de résidence seraient, en pratique, beaucoup moins nombreux que les affaires «ordinaires» dans lesquelles les décisions sont prises par la DPA chef de file «du domicile».

[193] Article 74, paragraphe 3.

Enfin, le principe de guichet unique pour les entreprises doit être considéré dans son propre contexte comme un élément capital contribuant à l'efficacité et à la cohérence globales du futur cadre relatif à la protection des données. Un système de protection des données beaucoup plus uniforme et des coûts de règlement des litiges réduits - étant donné que les litiges seraient en principe circonscrits à la juridiction de la DPA chef de file ou de l'établissement principal - seraient indéniablement plus avantageux pour les entreprises à travers l'Union européenne. Cependant, les citoyens tireront aussi parti de l'application plus cohérente d'un ensemble uniforme de règles de protection des données fixé en vertu de la proposition de règlement.

Par exemple, lorsqu'un citoyen sera affecté par un traitement de données effectué par un responsable du traitement établi dans différents pays, mais que toutes les décisions seront effectivement prises par l'établissement principal du responsable du traitement dans un autre État membre, la possibilité d'obtenir une décision unique d'une DPA ou un jugement valable et exécutoire dans tous les États membres constituera une avancée considérable par rapport à la situation actuelle.

Dans le même esprit, le guichet unique pour les entreprises réduit également la probabilité de procédures parallèles et de conflits de juridiction qui en résultent, étant donné qu'une procédure dans l'État membre de l'autorité chef de file suffirait normalement à faire valoir ses droits partout dans l'Union.

Comme cette discussion l'illustre, le concept de guichet unique, pour les entreprises ou les citoyens, soulève des questions susceptibles d'appeler quelques ajustements dans la proposition de règlement. C'est pour cette raison que différentes options sont toujours à l'examen. Cependant, il est évident que le résultat final sera fondé sur une étroite coopération entre les autorités plutôt que sur des compétences exclusives, et que la nécessité d'une protection effective et d'une plus grande efficacité recevra également, sans aucun doute, le poids qu'elle mérite.

D. Protection de la vie privée et «interopérabilité» plus globales

L'environnement numérique revêt une dimension de plus en plus mondiale, alors que l'internet et d'autres réseaux mondiaux permettent la circulation de données à travers le monde à chaque minute de chaque jour. Les aspects internationaux du règlement ont dès lors également reçu une attention considérable.

À cet égard, le règlement - à l'instar de la directive 95/46/CE, mais de manière plus marquée - ne se concentre pas essentiellement sur le *lieu* où les données se trouvent, mais plutôt sur la *responsabilité* du traitement des données et les *conséquences* du traitement des données pour les personnes concernées. C'est le champ d'application du règlement qui le fait ressortir le plus clairement: le règlement s'appliquera non seulement à tous les traitements

effectués dans le cadre des activités d'un établissement du responsable du traitement de données sur le territoire de l'Union, mais aussi lorsque des biens ou des services seront proposés sur le marché européen, ou à l'observation du comportement des personnes concernées au sein de l'Union, indépendamment du lieu à partir duquel le comportement sera contrôlé.[194] Dans toutes ces situations, le responsable du traitement devra veiller au respect des principes fondamentaux de la protection des données et des droits de la personne concernée, et sera soumis au contrôle d'autorités indépendantes.[195]

Lorsque le règlement s'appliquera, il exigera également que les données à caractère personnel ne soient pas transférées vers un pays tiers, à moins que la destination ne garantisse un niveau de protection adéquat ou n'offre des garanties adéquates par d'autres moyens. Ces dispositions ont été développées et simplifiées, si bien qu'il existera davantage d'options pour offrir une protection adéquate dans des situations spécifiques.[196] L'idée sous-jacente est que les données à caractère personnel ne devraient être transférées vers un pays tiers que si les droits des personnes concernées sont garantis. Parallèlement, ces dispositions se fondent sur un degré de pragmatisme raisonnable afin de permettre une interaction avec le reste du monde. Elles s'appliqueront donc également si les données à caractère personnel sont transférées vers des prestataires de services dans des pays tiers dans le cadre de l'informatique en nuage. Dans ces hypothèses, le responsable du traitement continuera d'assumer au moins la coresponsabilité du respect des exigences en matière de protection des données.[197]

Troisième élément, le règlement favorisera aussi la coopération avec les autorités en charge de la protection des données ailleurs dans le monde.[198] Il importe de collaborer efficacement

[194] Voir l'article 3. La Cour de justice a récemment statué, dans l'arrêt *Google Spain*, cité à la note de bas de page 45, que la directive 95/46/CE s'applique déjà à l'exploitation d'un moteur de recherche à partir d'un pays tiers via des filiales établies dans un État membre de l'UE. À cet égard, la Cour a jugé que l'opérateur de moteur de recherche était le responsable du traitement des données à caractère personnel effectué par le moteur de recherche et que les activités de la filiale - bien qu'elles se limitent à la vente d'espaces publicitaires - étaient indissociablement liées au traitement des données à caractère personnel résultant des recherches qui augmentaient la valeur de la publicité (voir l'arrêt Google Spain, points 33, 55 et 56). Ce faisant, la Cour a fait un pas important dans le sens que vise également le règlement.

[195] Dans son arrêt, la Cour relève qu'il appartient au responsable du traitement d'assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que son activité satisfait aux exigences de la directive (voir arrêt *Google Spain*, point 38). Cela vaut également lorsque cette activité est réalisée par des ordinateurs sur la base de programmes informatiques: une reconnaissance opportune de la responsabilité qui incombe aux responsables du traitement et de l'étendue de leurs obligations sur l'internet. Un des éléments clés pour la Cour est la nécessité de garantir «une protection efficace et complète» des droits fondamentaux (arrêt *Google Spain*, points 34, 38, 53 et 58). Il convient de souligner la confirmation par la Cour d'un détail important: la directive s'applique aux données à caractère personnel qui ont été déjà été publiées (arrêt *Google Spain*, point 30). Lors de la détermination des droits de la personne concernée au titre des articles 12 et 14 de la directive (notamment le droit à l'effacement des données et le droit de s'opposer au traitement des données à caractère personnel), la Cour renvoie précisément aux articles 7 et 8 de la charte (arrêt *Google Spain*, points 69, 81 et 97). Ce jugement peut donc être considéré comme une nouvelle preuve de l'incidence croissante de la charte sur l'application du droit existant.

[196] Articles 40 à 44.

[197] Article 24.

[198] Article 45.

avec les acteurs mondiaux sur l'internet. Comme cela a déjà été mis en avant à la section 5, partie C, cette avancée bénéficie d'une convergence croissante des principes et pratiques de protection des données à travers le monde, et est encouragée par les cadres du Conseil de l'Europe et de l'OCDE qui se chevauchent partiellement.

L'OCDE a récemment publié des lignes directrices révisées sur la protection de la vie privée, qui confirment fondamentalement l'approche suivie jusqu'à présent.[199] Ces lignes directrices révisées mettent également l'accent sur la nécessité de mesures pratiques visant à garantir le respect des principes de la protection des données et sur la coopération nécessaire entre les autorités chargées du respect de la vie privée.[200] La révision de la Convention 108 du Conseil de l'Europe va dans le même sens.[201]

Ensemble, tous ces éléments se conjugueront pour offrir une évolution progressive vers une «interopérabilité» mondiale des cadres relatifs au respect de la vie privée et à la protection des données. Bien qu'il s'avère plutôt aisé de recenser de nombreuses différences sur des détails, ces cadres sont de plus en plus propices à la synergie et à la convergence. Le règlement serait le cadre le plus développé au monde - dans le droit fil de la reconnaissance du droit à la protection des données comme droit fondamental consacré à l'article 8 de la charte -, mais il serait aussi cohérent avec les évolutions ailleurs. De plus, il se peut qu'il exerce une forte influence sur ces évolutions en temps utile, à l'image de la directive 95/46/CE par le passé. La révision de la directive offre donc aussi une occasion majeure d'assurer une protection de la vie privée et une interopérabilité plus globales.

Enfin, le règlement ne s'applique pas aux activités de surveillance entreprises par des pays tiers ou par les services compétents d'un État membre de l'Union. Il s'applique toutefois aux opérateurs et autres prestataires qui proposent leurs services sur le marché européen ou observent le comportement des personnes concernées au sein de l'Union, et peut donc offrir également des possibilités d'espionnage par d'autres acteurs.[202] Les obligations qui incombent au responsable du traitement en vertu du règlement serviraient, à cet égard, de pouvoir compensateur essentiel.

Dans ce contexte et dans un cadre plus large, il serait utile que le règlement contienne également une disposition abordant l'hypothèse d'une obligation légale imposée par un pays

[199] Disponibles (en anglais uniquement) à l'adresse suivante: http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines (dernière consultation le 31 mai 2014).
[200] La troisième partie sur l'application du principe de responsabilité et la sixième partie sur la coopération internationale et l'interopérabilité.
[201] Voir les informations disponibles à l'adresse suivante: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_FR.asp? (dernière consultation le 31 mai 2014).
[202] Article 3.

tiers qui exigerait des activités non conformes au droit de l'Union.[203] En principe, ces activités ne devraient pas être permises, sauf si un accord international venait à les autoriser ou si une autorité judiciaire ou de contrôle indépendante venait à octroyer une exemption. Cette disposition pourrait servir de régulateur indispensable dans les cas où des conflits de lois ou de politiques publiques internationaux seraient autrement susceptibles de se produire au détriment d'opérateurs économiques ou de l'intérêt général, voire les deux.

7. Autres questions

A. Marché intérieur et droits fondamentaux

La directive 95/46/CE a été adoptée sur la base juridique du marché intérieur afin de doter la protection des données au sein de l'UE d'un cadre juridique harmonisé. Néanmoins, l'angle des droits fondamentaux était visible d'emblée. La Cour de justice a mis en évidence le fait que la directive revêt un champ d'application très large et la charte exerce une influence grandissante sur son application dans la pratique. La révision de la directive s'inscrit aujourd'hui dans une autre perspective. L'article 16 du TFUE prévoit une base juridique générale pour une protection complète des données à caractère personnel dans tous les domaines stratégiques, et la charte s'applique aux institutions et aux États membres de l'Union européenne dès qu'ils agissent dans le cadre du droit européen.

Cette optique différente ne signifie pas que les considérations relatives au marché intérieur et les autres principes de politique publique pourraient ne plus jouer un rôle dans la manière dont la révision de l'actuel cadre juridique de l'Union en matière de protection des données est entreprise et, en effet, dans la structure et le contenu du nouveau cadre lui-même. Il est évident que le choix d'une proposition de règlement et nombre de ses caractéristiques principales sont fondés sur la nécessité d'une harmonisation plus large afin d'offrir une protection plus solide, plus efficace et plus cohérente des données à caractère personnel à travers l'Union européenne. Autrement dit, l'influence de la charte et la nécessité d'harmonisation et de cohérence à travers l'Union sont non seulement compatibles et complémentaires, mais elles se renforcent mutuellement aussi. Une protection plus solide et cohérente des données à caractère personnel est également dans l'intérêt du marché intérieur.

Cependant, nous pourrions toujours nous interroger sur le degré de flexibilité autorisé par l'article 16 du TFUE et sur les domaines dans lesquels l'influence de la charte pourrait imposer certaines limites que les responsables de l'élaboration des politiques publiques et le législateur de l'Union devraient respecter. Ces questions ne sont pas purement théoriques comme la discussion au sein du Conseil sur le guichet unique pour les entreprises l'a mis en

[203] Cette disposition faisait partie de la proposition de règlement de la Commission avant qu'elle ne soit supprimée à un stade ultérieur. Le Parlement et le Conseil envisagent également différentes versions d'une disposition similaire. Ses avantages iraient au-delà de la surveillance et pourraient également concerner d'autres domaines où les conflits de lois ou de politiques publiques internationaux, comprenant généralement des obligations juridiques d'accès aux informations dans d'autres juridictions, sont susceptibles de se produire.

évidence.[204] Les objections juridiques au principe de guichet unique ont été formulées afin de mettre en cause sa compatibilité avec la charte, et en particulier l'article 47 relatif au droit à un recours effectif et à un procès équitable. Bien que ces objections ne soient pas pleinement convaincantes, elles suggèrent l'existence effective de différentes limites que le législateur européen doit respecter.[205]

La Cour de justice a également démontré l'existence de telles limites. L'exemple le plus manifeste est tiré de la jurisprudence sur l'exigence d'«indépendance complète» des autorités de contrôle. En différentes occasions, la Cour a affirmé que l'exigence de contrôle indépendant constituait un «élément essentiel» de la protection des données à caractère personnel, qui résulte de l'article 8, paragraphe 3, de la charte, et de l'article 16, paragraphe 2, du TFUE.[206] Le législateur européen ne serait donc pas libre de réviser l'actuel cadre d'une manière qui ne serait pas compatible avec ces dispositions de droit primaire.

Une déduction similaire pourrait être tirée du récent arrêt de la Cour sur la position des exploitants de moteur de recherche. Étant donné que la portée des droits de la personne concernée à l'effacement des données la concernant et de s'opposer au traitement de celles-ci, au titre de l'actuelle directive, a été déterminée moyennant des références spécifiques aux articles 7 et 8 de la charte[207], il serait inconcevable de limiter la portée desdits droits sans tenir dûment compte des exigences de la charte concernant toute limitation de l'exercice des droits reconnus explicitement à l'article 8, paragraphe 2, ou, implicitement, à l'article 8, paragraphe 1, de la charte. En effet, la Cour n'était pas loin d'affirmer que ces droits sont (également) des «éléments essentiels» de la protection des données à caractère personnel au titre de l'article 8. Cela pourrait se reproduire à l'avenir dans des affaires ayant trait à d'autres parties de l'article 8.

De façon plus générale, il convient donc de garder à l'esprit les articles 7 et 8, ainsi que les autres dispositions pertinentes de la charte lors des discussions sur les détails du règlement et de leur adoption, et au final de les appliquer dans la pratique. C'est ici que la différence de nature entre le droit au respect de la vie privée et le droit à la protection des données à caractère personnel peut une fois encore jouer un rôle important. L'article 7 servirait alors essentiellement de garde-fou contre les ingérences dans la vie privée des personnes, tandis que l'article 8 servirait de garantie positive que les éléments essentiels de la protection des

[204] Voir la section 6, partie C, ci-dessus.
[205] Voir également, dans un contexte différent, l'arrêt *Digital Rights Ireland*, cité à la note de bas de page 97, point 47: «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 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».
[206] Voir note de bas de page 95.
[207] Voir note de bas de page 195.

données à caractère personnel, telles qu'énoncées dans cette disposition, sont délivrées de manière adéquate dans la pratique.

Ainsi, le règlement devrait être conçu et appliqué de telle sorte que le traitement des données à caractère personnel, par des acteurs publics ou privés, ne soit pas constitutif d'une ingérence excessive dans la vie privée des personnes, et que les éléments essentiels de la protection des données soient réunis aussi bien dans le secteur public que dans le secteur privé. Toute réduction de la portée ou du niveau de protection accordé au titre de l'actuelle directive pourrait dès lors rencontrer des difficultés justifiées au regard des articles 7 et 8 de la charte.

B. Responsabilité et conformité

À la section 5, parties B et C, nous avons indiqué qu'un des éléments les plus importants du règlement est le passage du contrôle préalable au contrôle ultérieur par les autorités en charge de la protection des données, et de la responsabilité nominale à la responsabilité accrue ou la responsabilisation des responsables du traitement. Un commentateur a qualifié cette transition de «révolution copernicienne dans la législation européenne en matière de protection des données».[208] Bien que ces termes puissent être exagérés, ils mettent assurément en avant un changement d'approche majeur visant à rendre la protection des données plus efficace dans la pratique.

Il importe de préciser ce que cette transition implique. Tout d'abord, l'actuel devoir pour les responsables du traitement de veiller au respect des principes matériels de la protection des données et de certains droits spécifiques des personnes concernées ne change pas. Tous ces éléments essentiels resteront intacts, sous réserve d'éclaircissements et d'améliorations apportés par le règlement.

Dans l'actuelle directive, ce devoir est complété par une obligation générale de notification préalable des traitements à la DPA compétente, obligation susceptible de faire l'objet d'exemptions, ou par une obligation de contrôle préalable en cas de traitements à risque.[209] Dans la pratique, cela s'est traduit non seulement par une très grande diversité d'un État membre à l'autre, en ce qui concerne aussi bien la portée des notifications que celle de l'exemption, mais aussi dans les pratiques nationales au titre de chaque catégorie pertinente. Plus important encore, les organisations responsables ont tendance à voir l'obligation principale dans la notification formelle, plutôt que dans l'obligation de se conformer aux principes de la protection des données. Cette tendance a mis excessivement l'accent sur le rôle des autorités chargées de la protection des données au détriment du rôle clé joué par les responsables du traitement pour garantir une bonne protection des données au sein de leur

[208] Voir Kuner, C., cité à la note de bas de page 128.
[209] Articles 18 à 20.

organisation. L'obligation de notifier au préalable les traitements individuels est désormais largement perçue comme une charge administrative inefficace et inutile.

Le règlement, en revanche, insiste davantage sur la mission des responsables du traitement. Par conséquent, ceux-ci devront non seulement veiller au respect des principes matériels et des droits des personnes concernées, mais aussi prendre toutes les mesures appropriées pour garantir la conformité, et vérifier et démontrer que ces mesures existent et restent effectives.[210] Ce principe de responsabilité devrait mener à une meilleure *gestion des données* dans la pratique, sous réserve de la mise en œuvre de l'approche basée sur les risques dite «progressive», abordée à la section 6, partie B. Les pouvoirs dont jouissent les autorités en charge de la protection des données pour la mise en application et l'infliction de sanctions en cas de non-respect ont également été étendus de manière significative.[211]

L'obligation distincte d'adopter des mesures appropriées et de prouver leur existence ainsi que leur efficacité continue a été conçue comme une incitation pour les responsables du traitement et comme un outil pour les autorités en charge de la protection des données aux fins du contrôle des pratiques en matière de gestion des données, sans nécessairement devoir procéder à une analyse chronophage des questions matérielles. Une approche basée sur les risques «progressive», telle que mentionnée ci-dessus, fonctionnerait bien dans ce contexte, tant pour les responsables du traitement que pour les autorités en charge de la protection des données. Elle nécessitera des orientations pratiques de la part de ces autorités, de préférence dans le cadre du comité européen de la protection des données, de manière à assurer une cohérence suffisante à travers l'Union européenne.

Il n'est pas difficile de prédire que les responsables du traitement seront enclins à rechercher des conseils d'experts sur la meilleure manière d'assurer la conformité au sein de leur organisation. Il s'ensuivra une demande croissante de professionnels dans le domaine du respect de la vie privée, ainsi que de produits et de services connexes, éventuellement soumis à une certification en vertu du règlement.[212] D'autre part, le règlement apportera davantage d'options différentes de mise en application, allant d'actions individuelles ou en nom collectif intentées par les parties intéressées à différentes interventions des autorités en charge de la protection des données, dans le cadre ou non d'un guichet unique, appuyées par le mécanisme de contrôle de la cohérence et le rôle du comité européen de la protection des données. En d'autres termes, les responsables du traitement seront à même d'assumer leurs responsabilités, le cas échéant avec l'aide d'autrui, et pourront faire l'objet de différentes actions de mise en application, en fonction du succès de leur mission.

[210] Article 22.
[211] Articles 53 et 79.
[212] Article 39.

En ce sens, le règlement conduira à une meilleure attribution des responsabilités et créera quelques incitations puissantes en faveur de la conformité, lesquelles se traduiront vraisemblablement par une protection plus efficace dans la pratique.

C. Contrôle indépendant et cohérence

L'exigence de contrôle indépendant a été mentionnée ci-dessus à plusieurs reprises comme un «élément essentiel» du droit à la protection des données, de même que la nécessité d'une plus grande cohérence comme condition d'une effectivité accrue de ce droit à travers l'Union européenne. Ces exigences sont-elles néanmoins pleinement compatibles entre elles? À première vue, il pourrait bien s'agir d'un véritable paradoxe dans la gouvernance de la protection des données au sein de l'Union européenne.

La jurisprudence de la Cour dispose que l'exigence d'une «indépendance complète» signifie qu'une autorité de contrôle doit être exempte de *toute* influence extérieure.[213] De toute évidence, il n'est pas exclu que ces autorités puissent coopérer entre elles et aboutir à un consensus sur certaines questions. Cependant, en cas de désaccord, la question de savoir qui prend une décision contraignante suscitera nécessairement des problèmes épineux. Si une minorité devait être liée par le point de vue d'une majorité, cela équivaudrait à une influence externe directe, difficilement compatible avec la notion d'indépendance complète. Si, d'autre part, chaque autorité de contrôle devait être libre de suivre son propre point de vue, il serait impossible d'obtenir une véritable cohérence sur un quelconque sujet.

Il convient de noter que le mécanisme de contrôle de la cohérence prévu par la proposition de règlement n'a pas pour vocation de conduire à une décision contraignante, mais à un avis *consultatif*, à la lumière duquel la DPA compétente devrait reconsidérer sa position.[214] Si la DPA suit l'avis consultatif, pas de problème. Dans le cas contraire, deux options principales se présentent en théorie.

Conformément à la première option, la DPA compétente doit motiver sa position et expliquer pourquoi elle ne suit pas l'avis consultatif. Cette option entraînerait indubitablement un examen plus étroit de la mesure par les parties intéressées et toute juridiction saisie ultérieurement. Elle respecterait pleinement l'indépendance, en ne créant qu'une pression procédurale, mais conduirait en revanche à une cohérence très limitée, peut-être uniquement après un jugement définitif par la Cour de justice.

La deuxième option consiste à faire entrer la procédure de cohérence dans une nouvelle phase. À cet égard, la Commission avait envisagé de jouer elle-même un rôle de plus en plus actif, tout d'abord par la soumission d'un avis, qui demanderait à l'autorité compétente qu'elle reconsidère sa position encore plus sérieusement, deuxièmement par la suspension de

[213] Voir les notes de bas de page 51 et 52.
[214] Article 58.

la mesure à l'examen, et enfin, par le règlement plus général de l'affaire de manière contraignante au travers de l'adoption d'un acte d'exécution.[215] Cette approche a suscité de nombreuses critiques la jugeant inappropriée. Bien que la Commission soit également tenue d'agir en toute indépendance en vertu des traités[216], cette exigence poursuit un objectif différent et ne suffirait pas à justifier une intervention directe dans une affaire soumise à une autorité indépendante.

Ces constats ont poussé à repenser la manière dont les autorités indépendantes pourraient coopérer pour atteindre des résultats positifs et cohérents. Il a été proposé que les problèmes présentant une nature purement ou majoritairement locale - tous les acteurs résidant dans le même pays ou tous les problèmes survenant dans le cadre d'une législation locale - soient être laissés entièrement aux autorités en charge de la protection des données compétentes à l'échelle locale. Si plus d'une juridiction est concernée - soit parce que le responsable du traitement possède des établissements dans différentes juridictions ou que des personnes relevant de différentes juridictions sont affectées -, la première règle devrait alors être la coopération entre les autorités compétentes en vue d'atteindre une solution qui puisse être acceptée par tous. Dans ces circonstances, il pourrait y avoir lieu de désigner une autorité chef de file aussi pour les affaires dans lesquelles le responsable du traitement est établi dans une seule juridiction et des personnes relevant de différentes juridictions sont affectées. En effet, il se peut que le responsable du traitement ne possède absolument aucun établissement au sein de l'Union européenne et que des personnes soient affectées dans tous les États membres. Différents scénarios pourraient dès lors être envisagés pour la désignation d'une telle autorité chef de file. Néanmoins, tant que le résultat de la coopération sera obtenu au moyen d'un consensus dans un délai raisonnable, la question de l'indépendance ne posera aucun problème.

Si la coopération entre les autorités en charge de la protection des données concernées n'aboutit pas à un consensus dans un délai raisonnable, le problème devra être soumis pour discussion au comité européen de la protection des données. Si cette discussion donne lieu à un résultat approuvé par consensus, il n'y aura de nouveau aucun problème d'indépendance. Cependant, si une majorité domine, deux scénarios se profilent essentiellement. Le premier est que l'opinion majoritaire ne serait qu'un avis *consultatif*, que la DPA compétente devrait au moins examiner très attentivement. En cas de désaccord persistant, il existerait la possibilité d'un deuxième avis consultatif, qui devrait être adopté à une majorité qualifiée. Ce scénario suivrait l'approche d'une pression procédurale croissante, sans limiter le pouvoir décisionnel de la DPA compétente, mais il se fonderait également sur la présomption que le second avis consultatif serait très influent, sans pour autant statuer pleinement sur tous les détails d'une affaire.

[215] Articles 59 à 62.
[216] Article 17, paragraphe 3, du TUE.

Le deuxième scénario consisterait à introduire un mécanisme décisionnel à un différent niveau, par exemple dans le cadre même du comité européen de la protection des données. Cette option pourrait également entraîner des conséquences pour le réexamen judiciaire de toute décision et pourrait donner lieu à une centralisation non souhaitable. D'autres solutions possibles ont été suggérées, mais sans répondre tout à fait au problème d'une minorité dissidente ou d'un éventuel manque de cohérence.

Cela explique pourquoi les questions de gouvernance liées au mécanisme de contrôle de la cohérence, ainsi que l'architecture du guichet unique pour les entreprises, font partie des questions les plus complexes actuellement discutées, et que différentes solutions sont étudiées afin de trouver un compromis acceptable.

8. Observations finales

L'issue de l'actuelle révision de la directive 95/46/CE - et du cadre juridique de l'UE relatif à la protection des données de manière plus générale - n'est pas tout à fait claire, mais sa principale direction semble désormais irréversible et bien au-delà du point de non-retour. Quoi qu'il en soit, quelques conclusions peuvent être tirées à ce stade.

Le respect de la vie privée et la protection des données - plus précisément le droit au *respect* de la vie privée et le droit à la *protection* des données à caractère personnel - sont étroitement liés. Tous deux sont des expressions assez récentes d'une idée universelle qui revêt de solides dimensions éthiques: la dignité, l'autonomie et la *valeur unique* de chaque être humain. Cependant, ils présentent également des différences cruciales. La notion de «protection des données» a été élaborée afin d'offrir une protection juridique structurelle aux personnes contre l'utilisation inappropriée des technologies de l'information aux fins du traitement d'informations les concernant, *indépendamment* du fait que ce traitement relève du champ d'application du droit au respect de la vie privée ou non. L'ensemble de garanties qui en a découlé - essentiellement un système d'équilibre des pouvoirs, composé de conditions matérielles, de droits individuels, de dispositions procédurales et d'un contrôle indépendant - s'applique en principe à tout traitement de données à caractère personnel.

Cette approche a été définie par le Conseil de l'Europe dans la Convention 108, puis développée par l'Union européenne dans la directive 95/46/CE, parallèlement au droit au respect de la vie privée tel qu'énoncé à l'article 8 de la CEDH. Il convient de les distinguer, d'une part, du concept allemand d'«autodétermination en matière d'informations», qui met fortement l'accent sur le consentement de la personne concernée, et d'autre part, de l'approche adoptée par les lignes directrices de l'OCDE, basées sur la notion de «risque» comme condition *minimale* de la protection et supposant que tout traitement de données à caractère personnel est en principe légitime. Ces distinctions jouent un rôle important - mais souvent seulement implicite et insuffisamment reconnu - dans les discussions internationales.

Progressivement, l'Union européenne a repris le rôle du Conseil de l'Europe comme plateforme pour bâtir la protection des données. À cet égard, nous avons vu deux axes principaux: le premier porte sur le *renforcement* des droits au respect de la vie privée et à la protection des données, et le deuxième sur la nécessité de garantir une application plus *cohérente* de ces droits à travers l'Union européenne. Ces deux axes visent à garantir une protection *plus efficace* dans la pratique et une *diversité inutile* moindre dans la manière dont cette protection est assurée dans les États membres. L'influence grandissante de la charte des droits fondamentaux, tant dans la jurisprudence de la Cour de justice que dans la révision du cadre juridique actuel, répond à cette tendance à long terme. Cette évolution est de toute évidence opportune, dans la mesure où la nécessité d'une protection efficace des données à caractère personnel n'a jamais été aussi grande qu'aujourd'hui.

Cette distinction entre «vie privée» et «protection des données» est également importante pour la charte. L'article 7 relatif au droit au respect de la vie privée est un exemple classique de droit fondamental, dans lequel l'*ingérence* est soumise à des conditions strictes. L'article 8 relatif à la protection des données à caractère personnel est le prolongement de la Convention 108 et de la directive 95/45/CE en ce qu'il procure un système de protection plus proactif. Il convient donc de ne pas confondre la *portée* de l'article 8 - couvrant tous les traitements de données à caractère personnel - avec la question de savoir s'il y a eu *ingérence* dans le droit fondamental à la protection des données. Une telle ingérence ne se produit habituellement que si un ou plusieurs éléments principaux de l'article 8, paragraphes 2 et 3, n'ont pas été respectés. Cependant, il ne faut pas exclure que l'article 8, paragraphe 1, puisse être utilisé comme source pour d'autres exigences, déjà prévues dans la législation européenne sur la protection des données, mais pas encore explicitées dans la charte.

Dans sa jurisprudence récente, la Cour de justice a tendance à faire une «lecture combinée» des articles 7 et 8 de la charte. Comme nous l'avons expliqué, cette approche ne tient pas compte de la différence essentielle de nature entre ces deux dispositions et risque donc d'empêcher l'article 8 de produire tous ses effets. Cependant, la Cour semble toujours aux prises avec le véritable rôle de l'article 8 de la charte et recourt parfois à une terminologie différente.

La base générale de la révision de l'actuel cadre juridique, prévue à l'article 16 du TFUE offre une occasion historique de traduire les éléments principaux de l'article 8 dans un ensemble de règles plus efficaces et cohérentes applicable à travers l'Union européenne. Le règlement général sur la protection des données, voué à remplacer la directive 95/46/CE le moment venu, combine continuité et innovation. Un règlement directement contraignant apportera en principe davantage de cohérence, mais dans la pratique, il risque probablement d'autoriser une certaine souplesse en faveur de l'interaction avec le droit national, tout particulièrement dans le secteur public. L'innovation majeure est attendue dans les responsabilités accrues des responsables du traitement, bien que l'influence de cette transition

dépende de l'approche basée sur les risques dite «progressive» actuellement à l'examen. L'innovation peut également être attendue dans le domaine du contrôle et de la mise en application, tout particulièrement en ce qui concerne les détails du guichet unique pour les citoyens et dans d'autres mécanismes destinés à garantir que les autorités de contrôle indépendantes aboutissent à des résultats cohérents. Enfin, la portée territoriale du règlement inclura vraisemblablement les entreprises qui exercent leurs activités sur le marché européen depuis un établissement ailleurs dans le monde.

Dans la mesure où la charte s'applique toujours dans le champ d'application du droit de l'Union, elle s'appliquera également au cadre juridique qui sera finalement adopté sur la base de l'article 16 du TFUE. Cela nous pousse à nous interroger sur la marge d'appréciation dont le corps législatif disposera pour l'adoption de ces règles. Dans nos discussions, nous avons abordé plusieurs exemples de marge d'appréciation limitée, soit parce que l'article 8 de la charte a déjà fixé certaines exigences positives, soit parce que la charte doit également être respectée chaque fois que les règles régissant le traitement des données peuvent servir de fondement à une ingérence dans le droit au respect de la vie privée. Il se peut également que des problèmes surviennent au regard de la charte, si la portée ou le niveau de protection des nouvelles règles venaient à être plus limités ou inférieurs à ce que prévoit le cadre juridique actuel.

Pour conclure, nous avons vu que les questions de gouvernance liées au guichet unique pour les entreprises et au mécanisme de contrôle de la cohérence font partie des questions les plus complexes qui font toujours l'objet de discussions. Il sera indispensable de faire preuve de créativité et de pragmatisme à cet égard, afin de garantir que les éléments essentiels de l'article 8 de la charte puissent effectivement se traduire dans la pratique.