Peter Hustinx

Contrôleur européen de la protection des données

Le leadership européen en matière de respect de la vie privée et de protection des données[1]

Cet ouvrage, qui comporte des contributions sur la proposition de règlement général européen sur la protection des données, constitue une excellente occasion de mettre en lumière le rôle moteur de l'Europe dans le respect de la vie privée et la protection des données à caractère personnel. Ce rôle a évolué au cours des décennies; au niveau européen notamment, tout d'abord dans le cadre du Conseil de l'Europe, puis, plus tard, essentiellement dans le cadre de l'Union européenne. À cet égard, nous avons assisté à l'établissement d'une *distinction* croissante entre «le respect de la vie privée» et la «protection des données» comme concepts distincts, plus récemment dans la Charte des droits fondamentaux de l'UE. Simultanément, une attention croissante a été accordée au développement d'une protection *plus forte* et *plus efficace* de la protection des données à caractère personnel et d'une protection *plus cohérente* dans tous les États membres de l'UE. Ces différents éléments sont tous repris dans la proposition de règlement général sur la protection des données. Bien évidemment, la nécessité d'une protection forte, efficace et cohérente des données à caractère personnel n'a jamais été aussi forte et elle croîtra probablement encore au cours des années à venir.

1. 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 nous concernant – sont toutes deux des expressions relativement récentes issues d'une idée universelle porteuse de dimensions éthiques fortes: la dignité, l'autonomie et *la valeur unique* de chaque être humain. Ces notions impliquent également le droit de chaque individu à développer sa propre personnalité et à avoir voix au chapitre sur les questions qui peuvent avoir des effets directs sur lui. Cela explique deux caractéristiques qui apparaissent régulièrement dans ce contexte: la nécessité d'empêcher les *ingérences* indues dans les affaires privées, et la nécessité de garantir aux personnes physiques un *contrôle* adéquat des questions qui peuvent les concerner.

Le concept de «protection des données» a été développé il y a quarante ans pour fournir une protection juridique aux personnes physiques contre l'utilisation inappropriée des technologies de l'information pour traiter des informations les concernant. Il n'avait pas vocation à *empêcher* le traitement de ces informations ou à *limiter* le recours aux technologies de l'information en tant que telles. Bien au contraire, il visait à offrir des garanties dans les cas où les technologies de l'information seraient utilisées pour traiter des

[1] Cet article sera publié dans: "Hacia un nuevo régimen europeo de protección de datos / Towards a new European Data Protection Regime", Valencia 2015.

informations concernant des personnes physiques. Cela se fondait sur la conviction début selon laquelle un recours massif aux technologies de l'information à cette fin pourrait avoir de lourds effets sur les droits et intérêts des personnes physiques.

2. Ce n'est qu'après la deuxième guerre mondiale que le concept de «droit au respect de la vie privée» a émergé en droit international. Il est d'abord apparu sous une forme relativement faible à l'article 12 de la déclaration universelle des droits de l'homme, selon lequel nul ne sera l'objet d'immixtions *arbitraires* dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation.

Une protection plus substantielle a ensuite été accordée dans l'article 8 de la convention européenne des droits de l'homme (CEDH), selon lequel toute personne a droit au *respect* de sa vie privée et familiale, de son domicile et de sa correspondance et selon lequel il ne peut y avoir 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 pour garantir certains intérêts légitimes importants.

Si la mention du «domicile» et de «correspondance» pouvait s'appuyer sur les traditions constitutionnelles de nombreux pays dans le monde, comme héritage commun d'un développement déjà long, parfois vieux de plusieurs siècles, l'accent placé sur «le respect de la vie privée» et sur la «vie privée» était nouveau et constituait une réaction évidente à ce qui s'était passé au cours de la deuxième guerre mondiale.

L'étendue et les conséquences de cette protection ont été explicitées par la Cour européenne des droits de l'homme dans un ensemble d'arrêts. Dans l'ensemble de ces affaires, la Cour examine, en substance, s'il y a eu une *ingérence* dans l'exercice du droit au respect de la vie privée, et, le cas échéant, si cette ingérence avait une base juridique *adéquate* (c'est-à-dire claire, accessible et prévisible), et si cette ingérence était *nécessaire* et proportionnée aux intérêts légitimes en cause.

3. Au début des années 1970, le Conseil de l'Europe a conclu que l'article 8 de la CEDH présentait un certain nombre de lacunes au vu des nouveaux développements, notamment compte tenu du recours croissant aux technologies de l'information: ces lacunes concernaient les incertitudes quant à ce que recouvrait le concept de «vie privée», l'accent placé sur la protection contre les ingérences par les «autorités publiques» et l'absence de démarche plus proactive, ainsi que l'abus éventuel en matière d'utilisation des informations à caractère personnel par des sociétés ou par d'autres organismes pertinents du secteur privé.

Cela a abouti à l'adoption, en janvier 1981, de la convention pour la protection des données, également connue sous le nom de convention 108, qui a jusqu'à présent été ratifiée par

46 pays, dont la totalité des États membres de l'Union européenne, la plupart des États membres du Conseil de l'Europe et un État non membre[2]. Le but de cette convention est 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»), les «données à caractère personnel» étant définies comme «toute information concernant une personne physique identifiée ou identifiable («personne concernée»).

Cela signifie que le concept de «protection des données» est *plus large* que celui de la «protection de la vie privée» parce qu'il englobe également d'autres droits et libertés fondamentales, et tout type de données *sans qu'il soit tenu compte* de leur lien avec la vie privée, et, dans le même temps, *plus restreint* parce qu'il concerne simplement le traitement des informations personnelles, faisant ainsi abstraction d'autres aspects de la protection de la vie privée.

Dans ce contexte, il convient de noter que nombreuses activités des secteurs public ou privé sont actuellement liées, d'une manière ou d'une autre, à la collecte de données à caractère personnel et au traitement de celles-ci. Le véritable objectif de la convention est donc de protéger les personnes physiques (citoyens, consommateurs, travailleurs, etc.) contre la collecte, l'enregistrement, l'utilisation et la diffusion injustifiés des informations à caractère personnel les concernant. Cela peut également concerner leur participation aux relations sociales, publiques ou non, et impliquer de protéger la liberté d'expression, d'empêcher la discrimination injustifiée, et de promouvoir le «fairplay» dans les processus décisionnels.

4. La convention comporte quelques principes de base sur la protection des données auxquels chaque partie contractante doit donner effet dans son droit national. Ces principes constituent encore la base de toute législation nationale dans ce domaine. La convention *n'est pas* fondée sur l'idée selon laquelle le traitement des données à caractère personnel doit toujours être considéré comme une *ingérence* dans l'exercice de ce droit au respect de la vie privée, mais plutôt sur l'idée selon laquelle, aux fins de la *protection* de la vie privée et d'autres droits et libertés fondamentales, le traitement de données à caractère personnel doit *toujours* être réalisé dans le respect de certaines conditions juridiques. On citera par exemple le principe selon lequel les données à caractère personnel ne peuvent être traitées qu'à des fins légitimes spécifiées, et à condition que cela soit nécessaire pour atteindre ces objectifs, et ne sauraient être utilisées d'une manière incompatible avec ces objectifs.

Conformément à cette approche, les éléments fondamentaux de l'article 8 CEDH, comme l'ingérence dans l'exercice du droit au respect de la vie privée, uniquement sur une base

[2] L'Uruguay a été le premier État non membre à ratifier la Convention en avril 2013.

juridique adéquate et lorsque cela est nécessaire en vue d'atteindre un objectif légitime, ont été transposés dans un contexte plus large. En pratique, cela n'est possible que si le système d'équilibre des pouvoirs, exposé dans la convention (fondé sur l'existence de conditions matérielles, de droits individuels, de dispositions procédurales, d'un contrôle indépendant) est suffisamment flexible pour prendre en compte des contextes divers, et est appliqué avec pragmatisme et réalisme dans l'intérêt des personnes concernées et des autres parties prenantes. Dans le cadre de cette approche, le droit au respect de la vie privée, prévu à l'article 8 de la CEDH, continue de jouer un rôle important dans le contexte, *notamment* pour déterminer la légitimité de mesures spécifiques plus intrusives.

La convention a joué un rôle majeur dans l'élaboration des politiques législatives de nombreux États membres du Conseil de l'Europe. Dans ce contexte, la question de la «protection des données» a dès le départ été considérée comme une question d'importance structurelle majeure dans une société moderne, dans laquelle le traitement des données à caractère personnel joue un rôle toujours plus grand.

5. Quelques années seulement après l'adoption de la convention 108, la Cour constitutionnelle allemande a rendu un arrêt dans lequel elle consacrait un droit à «l'auto-détermination informationnelle» comme expression du droit au libre développement de la personnalité, garanti par l'article 2, paragraphe 1, de la constitution allemande. Dans ce contexte, tout traitement de données à caractère personnel est, en principe, considéré comme une ingérence dans l'exercice du droit à l'«autodétermination informationnelle», à moins que la personne concernée n'ait donné son consentement. Cette approche doit clairement être distinguée de celle suivie dans le cadre de la convention 108, et sur cette base (comme nous le verrons) dans la directive 95/46/CE et dans les dispositions pertinentes de la Charte de l'UE.

Quelques mois avant l'adoption de la convention 108, l'OCDE a adopté des lignes directrices sur la protection de la vie privée qui, même si elles sont dépourvues de caractère contraignant, ont également eu une influence importante, notamment dans les pays hors d'Europe, comme les États-Unis, le Canada, l'Australie et le Japon. Ces lignes directrices, qui contiennent un ensemble de principes de base élaborés en étroite collaboration avec le Conseil de l'Europe, étaient donc conformes aux principes de protection des données prévus par la convention 108. Toutefois, il existait également des différences subtiles, mais significatives sur le plan 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». Cela impliquait que la notion de «risque» constituait une condition *de seuil* pour la protection des

données, ce qui n'était pas pleinement compatible avec l'approche du Conseil de l'Europe fondée sur les droits fondamentaux. De surcroît, la nécessité de l'existence d'un objectif *légitime* et d'une base *juridique* pour traiter les données à caractère personnel était en tant que telle absente des lignes directrices. Ces deux éléments sont toujours hautement pertinents dans les discussions au plan mondial.

6. Même si le Conseil de l'Europe a connu un véritable succès en inscrivant «la protection des données» à l'ordre du jour et en exposant les principaux éléments d'un cadre juridique, il n'a pas connu le même succès lorsqu'il s'est agi de garantir une cohérence suffisante entre les États membres. Certains États membres étaient en retard pour mettre en œuvre la convention 108, et ceux qui l'ont effectivement mise en œuvre sont parvenus à des résultats relativement différents, imposant même parfois des restrictions sur la circulation de données à destination d'autres États membres.

La Commission européenne craignait donc sérieusement que ce manque de cohérence entrave le développement du marché interne dans un certain nombre de domaines – y compris la libre circulation des personnes et des services – où le traitement des données à caractère personnel devait jouer un rôle de plus en plus important. À la fin de l'année 1990, elle a donc présenté une proposition de directive en vue d'harmoniser les législations nationales sur la protection des données dans le domaine privé et dans la plupart du secteur public. Après quatre années de négociations, cette proposition a abouti à l'adoption de l'actuelle directive 95/46/CE, qui poursuit un double objectif: garantir un niveau élevé de protection des données à caractère personnel équivalent dans l'ensemble des États membres, et garantir la libre circulation des informations entre États membres, sous réserve de l'existence de garanties convenues.

À cet égard, la directive s'est fondée sur les principes de base de la protection des données, exposés dans la convention 108 du Conseil de l'Europe. Dans le même temps, elle a précisé ces principes et les a complétés par des exigences et des conditions supplémentaires. Toutefois, dans la mesure où la directive a adopté des concepts formulés en des termes généraux et des normes ouvertes, elle accordait encore aux États membres un pouvoir d'appréciation relativement large au moment de la transposition. La directive a donc abouti à une cohérence accrue entre États membres, sans toutefois aboutir à l'adoption de solutions identiques ou totalement cohérentes.

De surcroît, la directive a été adoptée alors que l'internet n'était encore que peu répandu, et il est évident que le besoin d'une protection plus forte et d'une cohérence accrue n'a fait qu'augmenter au cours des dernières années. Sur ces deux aspects, la proposition de règlement général sur la protection des données vise à mettre en place les étapes suivantes.

7. Alors même que la directive a été adoptée pour garantir le bon fonctionnement du marché intérieur, son histoire et son contexte véhiculaient également un message plus large. Depuis, la Cour de justice de l'Union européenne a jugé à maintes reprises que cette directive avait un champ d'application large et s'appliquait également au secteur public des États membres[3]. Cette origine des droits fondamentaux est devenue plus visible au fil des ans.

L'adoption de la charte des droits fondamentaux de l'UE, qui était au départ un document politique, en décembre 2000, a permis des développements supplémentaires dans cette direction. L'une des nouveautés de la charte était qu'*en plus* du droit au respect de la vie privée, elle contenait une reconnaissance explicite du droit à la protection des données à caractère personnel dans une disposition distincte. Conformément à l'article 7, relatif au «*respect de la vie privée et familiale*», «[t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications».

Conformément au premier paragraphe de l'article 8 relatif à la «*protection des données à caractère personnel*», «[t]oute personne a droit à la protection des données à caractère personnel la concernant». Conformément au deuxième paragraphe du même article, «[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 «[t]oute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification». Conformément au troisième paragraphe, «[l]e respect de ces règles est soumis au contrôle d'une autorité indépendante».

8. Les droits garantis à l'article 7 de la Charte correspondent à ceux qui sont garantis par l'article 8 de la convention européenne des droits de l'homme. Tous deux sont des exemples typiques de droits fondamentaux classiques, pour lesquels l'*ingérence* fait l'objet de conditions strictes. L'article 8 est largement fondé sur la directive 95/46/CE et sur la convention 108 du Conseil de l'Europe.

Comme exposé précédemment, le droit à la protection des données à caractère personnel a été conçu par le Conseil de l'Europe et énoncé dans la convention 108 afin de garantir une protection *proactive* des droits et libertés des personnes physiques, par rapport à tout traitement de données à caractère personnel les concernant, indépendamment du point de savoir si ce traitement constitue ou non une ingérence dans l'exercice du droit au respect de la vie privée. Le but était de créer un système «d'équilibre des pouvoirs» afin de fournir une protection *structurelle* aux personnes physiques dans une large gamme de situations, dans le secteur privé comme dans le secteur public.

[3] Arrêt de la Cour du 20 mai 2003, *Österreichischer Rundfunk*, affaires jointes C-465/00, C-138/01 et C-139/01, Rec. p. I-04989, points 41-43 ; du 6 novembre 2003, *Bodil Lindqvist*, C-101/01, Rec. p. I-12971, points 39-41. Voir également Arrêt de la Cour (grande chambre) du 16 décembre 2008, *Huber*, C-524/06, Rec. p. I-09705 ; arrêt du 7 mai 2009, *Rijkeboer*, C-553/07, Rec. p. I-03889.

La directive 95/46/CE s'est fondée sur la convention 108 comme point de départ pour l'harmonisation des législations relatives à la protection des données au sein de l'Union européenne, et l'a précisé de différentes manières. Dans ce cadre, figuraient, en tant que principaux éléments structurels de la protection des données, les principes matériels de protection des données, les obligations des responsables du traitement, les droits des personnes concernées et la nécessité d'un contrôle indépendant. Toutefois, la nature de la protection des données entendue comme système «d'équilibre des pouvoirs» visant à fournir une protection dès lors que les données à caractère personnel sont traitées, n'a pas été modifiée. En d'autres termes, les articles 7 et 8 n'ont pas le même caractère et doivent être clairement distingués.

9. La convention qui a préparé la charte avant son adoption envisageait également d'inclure un droit à l'autodétermination informationnelle dans l'article 8, mais cette idée a été rejetée. À la place, elle a décidé d'inclure un droit à la protection des données à caractère personnel, de préserver les principaux éléments de la directive 95/46/CE. Ainsi, les éléments essentiels prévus à l'article 8, paragraphe 2, et à l'article 8, paragraphe 3, correspondent aux principes-clés de la directive 95/46/CE, comme le traitement licite et loyal, la limitation des objectifs poursuivis, les droits d'accès et de rectification, et le contrôle indépendant.

De plus, il ne saurait être exclu que la Cour de justice de l'Union européenne trouve d'autres éléments de protection des données qui n'ont pas été mentionnés dans l'article 8, paragraphes 2 et 3, mais qui figurent dans la directive 95/46/CE et peuvent être interprétés comme étant suggérés à l'article 8, paragraphe 1, de la charte. Ces éléments pourraient également aider à renforcer ceux qui sont déjà explicitement prévus, et développer davantage l'impact du droit à caractère général exprimé à l'article 8, paragraphe 1.

En tout état de cause, cela signifie que le *champ d'application* de l'article 8 – qui concerne tous les traitements de données à caractère personnel – ne doit pas être confondu avec la question de savoir si le droit fondamental garanti par l'article 8 a fait ou non l'objet d'une *ingérence*. L'ingérence au sens de l'article 8 ne naît pas du simple fait que des données à caractère personnel sont traitées. Une telle ingérence ne peut être établie que si un ou plusieurs des éléments principaux du droit à la protection des données (comme la nécessité d'un «fondement légitime prévu par la loi» ou d'un «contrôle indépendant») n'a pas été respecté.

10. L'entrée en vigueur du traité de Lisbonne en décembre 2009 a eu un impact énorme sur le développement de la législation de l'UE en matière de protection des données.

En premier lieu, la Charte a reçu la même valeur juridique que les traités, aux termes de l'article 6, paragraphe 1, du traité sur l'Union européenne. Elle est donc devenue un instrument à caractère contraignant, non seulement à l'égard des institutions et organes de l'Union européenne, mais également des États membres qui agissent dans le cadre du droit de l'Union. Le droit à la protection des données à caractère personnel a été, de plus, spécifiquement mentionné à l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE) comme faisant partie des principes généraux de Union européenne. Cela signifie que certains des principaux éléments de la directive 95/46/CE relèvent désormais du droit primaire de l'Union.

En second lieu, l'article 16, paragraphe 2, TFUE prévoit désormais un fondement juridique pour l'adoption par le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, de règles «relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel» par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la «libre circulation de ces données». Enfin, comme l'article 8, paragraphe 3, de la charte, l'article 16, paragraphe 2, souligne également que le respect de ces règles est soumis au contrôle d'autorités indépendantes.

La terminologie utilisée dans le texte principal rappelle la directive 95/46/CE, mais le champ d'application de cette nouvelle base juridique, qui a été formulée comme une obligation, va en réalité bien au-delà du marché intérieur et couvre en principe l'intégralité des politiques européennes. Le terme «règles» permet le recours à des directives et des règlements directement applicables, et le choix entre ces deux types d'actes semble désormais être essentiellement un choix politique.

11. La base générale de révision du cadre juridique actuel de l'article 16 TFUE constitue une occasion historique de prévoir les principaux éléments de l'article 8 de la Charte dans un ensemble de règles plus efficace et plus cohérent dans toute l'Union européenne.

La proposition de règlement général sur la protection des données, qui va remplacer la directive 95/46/CE en temps utile, allie continuité et innovation. Tous les principes et concepts de base ont été confirmés, et n'ont en règle générale fait l'objet que de quelques éclaircissements. Le règlement continuera à avoir un large champ d'application, lequel inclura également, selon toute vraisemblance, le secteur public, et garantira des droits renforcés pour les personnes concernées, des obligations plus fortes pour les responsables du traitement des données, et des modalités plus robustes de contrôle et de mise en œuvre, y compris des amendes administratives de plusieurs millions d'euros. Il s'agit là d'une reconnaissance de l'importance croissante de la protection des données dans l'économie numérique.

Un règlement directement contraignant apportera en principe une cohérence bien plus grande, mais il offrira sans doute également en pratique, une certaine souplesse pour interagir avec le droit national, notamment dans le secteur public. La plus grande innovation est attendue dans l'accroissement des responsabilités des responsables du traitement, bien que l'impact de ce changement dépende de «l'approche progressive de l'évaluation des risques» qui est actuellement en discussion. On attend également de l'innovation dans le domaine du contrôle et de la mise en œuvre, notamment en ce qui concerne les caractéristiques des guichets uniques pour les citoyens et pour les entreprises et dans le cadre d'autres mécanismes, afin de garantir des résultats cohérents des autorités de contrôle indépendantes.

Le champ d'application territorial du règlement devrait inclure les sociétés qui exercent une activité économique sur le marché européen depuis un établissement situé ailleurs dans le monde. Dans un arrêt récent, sur la base de la directive actuelle, la Cour de justice a fait une avancée intéressante dans cette direction, en reliant les activités commerciales d'un établissement d'un important moteur de recherche en Espagne avec celles du moteur de recherche lui-même, établi aux États-Unis.[4]

12. La proposition de règlement n'a, bien évidemment, pas été préparée de manière isolée. Le Conseil de l'Europe comme l'OCDE ont également procédé à une révision de leur cadre juridique et les résultats semblent tous aller dans le même sens, à savoir le renforcement de l'efficacité de la protection des données dans la pratique. Le règlement (une fois qu'il sera adopté, très probablement au cours de l'année 2015) devrait donc, en tant que point de référence majeur, avoir un fort impact, à la fois pour les autres pays du monde, et pour les acteurs économiques dont le succès peut dépendre de la capacité à garantir une protection efficace des données à caractère personnel de leurs clients et du respect de la vie privée de ceux-ci.

[4] Arrêt de la Cour (grande chambre), du 13 mai 2014, C-131/12, *Google Spain*, non encore publié, points 55-56.