# (FUTURE) INTERACTION ENTRE LES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES ET LES INSTITUTIONS NATIONALES DES DROITS DE L'HOMME [*]

**Peter J. Hustinx**[**]

## 1. INTRODUCTION

Conformément à la directive 95/46/CE, tous les États membres de l'UE ont des autorités nationales responsables de contrôler le respect des lois relatives à la protection des données. Néanmoins, la transposition de la directive dans les législations nationales varie considérablement. Cela se traduit par des divergences et des lacunes qui ont été mises en lumière par l'Agence des droits fondamentaux de l'UE et également dans la récente jurisprudence de la Cour européenne de justice. En janvier 2012, la Commission européenne a présenté un ensemble de propositions visant à mettre à jour et renforcer le cadre juridique actuel relatif à la protection des données dans l'UE. Cette révision aura également un impact sur la portée de l'interaction utile entre les autorités chargées de la protection des données et les institutions nationales des droits de l'homme.

L'émergence du droit à la protection des données à caractère personnel («protection des données») en tant que droit fondamental distinct – étroitement lié au droit au respect de la vie privée, mais avec ses propres caractéristiques – est une évolution propre au paysage européen des droits de l'homme. Si des législations similaires ont été développées dans d'autres régions du monde – basées sur des théories sur le respect de la vie privée, un traitement équitable des données, la protection des consommateurs, ou simplement la nécessité de créer des conditions appropriées pour la croissance économique – les évolutions en Europe ont été influencées par la conviction précoce que l'essor de la société de l'information aurait un tel impact sur l'exercice des droits fondamentaux existants et des libertés des citoyens qu'une approche plus proactive et systématique était nécessaire.

Les premières mesures ont été prises dans le cadre du Conseil de l'Europe et ont débouché sur l'adoption en 1981 d'une Convention sur la protection des données, également connue comme la Convention 108, avec des principes fondamentaux pour le traitement des données à caractère personnel dans les fichiers de données automatisés ou structurés d'une autre façon.[1] Le terme «protection des données» a été défini comme la protection des libertés et droits fondamentaux des personnes physiques, *en particulier* de leur droit à la vie privée, à l'égard du traitement des données à caractère personnel.[2] La Convention dépasse donc la portée de l'article 8 de la Convention européenne des droits de l'homme (CEDH),[3] et s'applique, en principe, à toutes les

---

[*] Publié dans: «National Human Rights Institutions in Europe - Comparative, European and International Perspectives», Jan Wouters et Katrien Meuwissen (eds.), Cambridge 2013, p. 157-172.

[**] M. Hustinx est le Contrôleur européen de la protection des données (CEPD).
Contact: edps@edps.europa.eu; Site internet: www.edps.europa.eu

[1] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28.I.1981 (ci-après la Convention 108).

[2] Convention 108, article premier.

[3] Article 8 «Droit au respect de la vie privée et familiale»:
1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

données à caractère personnel, indépendamment du droit à la vie privée. Les principes de la Convention 108 prévoient des exigences de fond pour les responsables du traitement des données, des droits spécifiques pour les personnes concernées et des modalités pour la supervision des institutions, le contrôle de l'application et la coopération internationale. La Convention a été ratifiée par plus de 40 États, y compris tous les États membres de l'UE.

Lorsque la Convention 108 a été mise en œuvre dans le droit national, il est rapidement devenu évident que la généralité des termes de ses dispositions donnait lieu à des divergences entre les législations nationales relatives à la protection des données. En même temps, le développement d'une société de l'information exigeait davantage d'harmonisation et de cohérence entre les législations nationales que la Convention ne le permettait. De fait, l'UE a été amenée à s'impliquer, ce qui a débouché sur l'adoption de la directive 95/46/CE relative à la protection des données, qui prend la Convention comme point de départ tout en y apportant des précisions à différents égards, notamment en exigeant qu'une ou plusieurs autorités de protection des données exercent en toute indépendance leur mission de surveillance et de contrôle de l'application.[4]

L'étape suivante a été l'adoption de la Charte des droits fondamentaux de l'Union européenne en 2000,[5] limitée dans un premier temps à une portée politique. Bien qu'elle soit largement fondée sur la Convention européenne des droits de l'homme, elle contient également des innovations, notamment la reconnaissance d'un droit à la protection des données à caractère personnel (article 8), en plus du droit au respect de la vie privée et familiale (article 7). L'article 8 mentionne explicitement certains des principaux éléments du droit à la protection des données à caractère personnel, tels qu'ils sont développés dans la directive 95/46/CE:

> **Protection des données à caractère personnel**
> 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

L'étape finale a été l'entrée en vigueur du traité de Lisbonne, à la fin de l'année 2009,[6] qui a transformé la Charte en un document juridiquement contraignant,[7] et introduit une base juridique horizontale pour la législation sur la protection des données, ne dépendant plus des besoins du marché intérieur, mais reflétant pleinement la nature de

---

2. 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 à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

[4] 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* 281/31, 23 novembre 1995. Voir en particulier l'article 28.

[5] Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), *JO L* 364/1, 18 décembre 2000 (ci-après la Charte).

[6] Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne (2007/C 306/01), *JO L* 306/1, 17 décembre 2007.

[7] Version consolidée du traité sur l'Union européenne, *JO L* C 115/19, 9 mai 2008 (ci-après: TUE). Voir l'article 6.

la protection des données en tant que droit fondamental, parmi les principes généraux de l'Union.[8] Cela a marqué la confirmation d'une évolution juridique de plusieurs décennies.

## 2. SURVEILLANCE INDÉPENDANTE

L'existence des autorités de protection des données est une constante du droit européen en matière de protection des données depuis le début, mais il a fallu du temps avant que le principe de contrôle *indépendant* ne devienne un principe constitutif. L'article 8 de la Charte le prévoit désormais comme nous venons de le voir, et l'article 16 TFUE également dans des termes très similaires. L'article 28 de la directive 95/46/CE, comme nous le verrons,[9] aborde le sujet plus en détails.

Rétrospectivement, il est surprenant de voir que, malgré l'expérience acquise en Allemagne, en Suède et en France, la notion d'«autorité chargée de la protection des données» n'a joué qu'un rôle très limité dans la Convention 108 du Conseil de l'Europe lorsque celle-ci a été conclue en 1981. Selon l'article 4 de la Convention, chaque partie a pour principale obligation de prendre «dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données» énoncés dans la Convention. Aux termes de l'article 10, chaque partie s'engage à établir «des sanctions et recours appropriés» visant les violations de ces principes de base. Le rapport explicatif indique clairement qu'il est nécessaire de garantir une «protection efficace», mais laisse à chaque partie le soin de déterminer librement les moyens d'y parvenir.[10] L'existence d'autorités de contrôle n'est mentionnée que comme la spécificité de certains droits nationaux. Les rédacteurs de la Convention étaient de toute évidence réticents à imposer cette disposition à toutes les parties comme une exigence légale fondamentale.

Cette situation a évolué avec l'adoption de la directive européenne 95/46/CE relative à la protection des données. L'article 28 de la directive a introduit l'obligation pour chaque État membre de disposer d'une ou de plusieurs autorités de contrôle chargées de surveiller l'application des dispositions relatives à la protection des données en exerçant leur mission «en toute indépendance». Le considérant (62) du préambule souligne que «l'établissement, dans les États membres, d'autorités de contrôle exerçant leurs fonctions en toute indépendance est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel». Les termes «exerçant …. en toute indépendance» constituent une formule de compromis choisie pour assurer une certaine flexibilité. Il est cependant difficile d'imaginer un exercice «en toute indépendance» en l'absence de garanties institutionnelles suffisantes. Cet aspect est d'ailleurs en cause dans une affaire portée devant la CJUE impliquant l'Allemagne, sur laquelle nous reviendrons.[11]

Aux termes de l'article 28 de la directive, les autorités de contrôle doivent également être dotées de certains pouvoirs tels que des pouvoirs consultatifs, des pouvoirs d'investigation, des pouvoirs effectifs d'intervention, le pouvoir d'ester en justice ou de porter des violations à la connaissance de l'autorité judiciaire, de traiter des plaintes, etc. Cela semble leur assurer une position centrale. Toutefois, ces autorités

[8] Version consolidée du traité sur le fonctionnement de l'Union européenne, *JO L* C 115/47, 9 mai 2008 (ci-après: TFUE). Voir article 16.
[9] Voir *infra* section 2.
[10] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Rapport explicatif, paragraphe 60.
[11] Voir *infra*, section 4.

ne décident pas en dernier ressort, et leurs décisions peuvent faire l'objet d'un recours juridictionnel.

L'adoption de la directive a conduit à l'élaboration d'un protocole additionnel à la Convention 108, qui reprend en substance tous les éléments de l'article 28 de la directive.[12] Le préambule du protocole additionnel indique clairement que les «autorités de contrôle exerçant leurs fonctions en toute indépendance sont un élément de la protection effective des personnes à l'égard du traitement des données à caractère personnel». Le rapport explicatif conclut même que les autorités de la protection des données «sont devenues partie intégrante du système de contrôle de la protection des données dans une société démocratique».[13] Ce rapport insiste également sur la notion de «protection efficace» et sur le rôle joué par les autorités de contrôle pour la garantir.[14]

Tout cela signifie, à la lumière de l'article 8 de la Charte et de l'article 16 TFUE, que le principe de «contrôle indépendant» et l'existence d'«autorités de contrôle indépendantes» sont devenus – tout au moins au niveau européen – les éléments constitutifs du droit à la protection des données dans une société démocratique. Cette approche est basée sur leur mission visant à «veiller au respect» et demeure étroitement liée à la notion de «protection efficace».

### 3. DIVERSITÉ ET LACUNES

Conformément à la directive 95/46/CE, tous les États membres de l'UE ont des autorités nationales chargées de surveiller le respect des lois relatives à la protection des données. Toutefois, la transposition de la directive dans les législations nationales varie considérablement. Cela a donné lieu à des divergences et lacunes qui ont été également soulignées dans un rapport publié par l'Agence des droits fondamentaux de l'UE (FRA)[15] en mai 2010.

Pour commencer, il convient de noter qu'une certaine diversité est inévitable et résulte simplement des traditions juridiques différentes qui existent dans les États membres. La directive laisse aux États membres une grande marge de manœuvre pour décider de la nature et de la structure qui leur paraissent les plus appropriées pour l'autorité de contrôle. Les autorités chargées de la protection des données existent donc sous différentes formes: des commissions petites ou grandes, des commissaires individuels, élus ou nommés, éventuellement par le gouvernement national ou le parlement, …etc.

Néanmoins, comme la FRA l'a clairement indiqué dans son rapport, l'actuelle disparité dépasse de loin le stade de l'inévitable diversité et, qui plus est, s'accompagne

[12] 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, STE n° 181, Strasbourg, 8 novembre 2001 (entrée en vigueur: 1er juillet 2004).

[13] 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, STE n° 181, rapport explicatif, Préambule, paragraphe 5.

[14] *Ibidem*, Préambule; paragraphe 8; paragraphe 13; paragraphe 16; paragraphe 17; paragraphe 24.

[15] Voir: FRA, « La protection des données à caractère personnel dans l'Union européenne: le rôle des autorités nationales chargées de la protection des données, Renforcement de l'architecture des droits fondamentaux au sein de l'UE II», Luxembourg, Office des publications de l'Union européenne, 2010.

de lacunes plutôt graves.[16] Les principales conclusions du rapport ont été résumées comme suit par la FRA:[17]

> **Connaissance des droits**
> Sept répondants sur dix dans le cadre d'une récente enquête Eurobaromètre n'étaient pas au courant qu'il existe une autorité chargée de la protection des données dans leur pays.
> **Pouvoirs limités**
> Il est fréquent que les autorités chargées de la protection des données ne disposent pas de la totalité des pouvoirs d'investigation et d'intervention ni de la capacité de donner des conseils juridiques ou d'ester en justice.
> **Non-respect**
> Dans de nombreux États membres, on observe un large mépris de l'obligation de s'enregistrer auprès de l'autorité chargée de la protection des données avant de s'engager dans des opérations de traitement des données.
> **Manque d'indépendance**
> Le manque d'indépendance de plusieurs autorités chargées de la protection des données à l'égard du gouvernement, dans l'UE, constitue un problème majeur pour leur crédibilité. Une modification des procédures de nomination/désignation (…) dans le cadre de la réforme législative pourrait résoudre le problème du manque d'indépendance.
> **Insuffisance des ressources financières et du personnel**
> Les autorités chargées de la protection des données [dans un certain nombre d'États membres] sont incapables d'exécuter l'intégralité de leurs tâches en raison des ressources économiques et humaines limitées qui sont à leur disposition.
> **Absence d'indemnisation et de sanctions**
> Une réforme législative est nécessaire pour conférer aux autorités chargées de la protection des données un rôle actif dans les procédures conduisant à des sanctions et indemnisations. Lorsque les autorités de protection des données ont les pouvoirs concernés, elles ont également besoin des ressources correspondantes pour être en mesure de les exercer efficacement. (...)

Le rapport de la FRA mentionne également des exemples de bonnes pratiques,[18] mais la diversité et les lacunes exposées dans le rapport demeurent plutôt préoccupantes.

### 4. EXIGENCE DE L'EXERCICE DES FONCTIONS «EN TOUTE INDÉPENDANCE»

La Cour de Justice de l'Union européenne (CJUE) s'est entretemps également exprimée sur l'exigence d'«indépendance» telle qu'énoncée à l'article 28 de la directive 95/46/CE.

L'arrêt du 9 mars 2010 de la CJUE dans l'affaire 518/07 (*Commission contre la République fédérale d'Allemagne*) concernait les autorités allemandes chargées de superviser le traitement des données à caractère personnel par des *organismes non publics* au niveau régional. Dans tous les États, ces autorités étaient soumises à la tutelle de l'État. La Commission européenne, au tribunal, soutenue par le Contrôleur européen de la protection des données (CEPD), considérait qu'exercer ses fonctions «en toute indépendance» à l'article 28 de la directive 95/46/CE signifie qu'une autorité

[16] *Ibidem*, p. 42 à 45.
[17] Voir le site internet de la FRA: http://fra.europa.eu/fr/publication/2012/data-protection-european-union-role-national-data-protection-authorities.
[18] FRA, loc. sit. *supra* note 15, pp. 47 à 48.

de contrôle doit être libre de *toute* influence extérieure, quelle qu'elle soit.[19] La République fédérale d'Allemagne pensait seulement à l'indépendance *fonctionnelle* – c'est-à-dire de ceux soumis au contrôle – mais n'excluait pas la tutelle de l'État.[20]

La CJUE a tranché en faveur de la Commission – en disant, en substance, que l'expression «en toute indépendance» signifie bien «en toute indépendance». Mais son analyse comprend quelques messages intéressants. Le point de départ de la Cour est que la signification de l'exigence se trouve dans le libellé de l'article 28 et les objectifs et l'économie de la directive.

Quant au *libellé* de l'article 28, la Cour mentionne qu'en matière d'organe public, le terme «indépendance» désigne normalement «un statut qui assure à l'organe concerné la possibilité d'agir en toute liberté, à l'abri de toute instruction et de toute pression».[21] En outre, selon la Cour, la notion d'«indépendance» renforcée par l'adjectif «toute», implique un «pouvoir décisionnel soustrait à toute influence extérieure à l'autorité de contrôle, qu'elle soit directe ou indirecte».[22]

Quant aux *objectifs* de la directive 95/46, la Cour considère que cette dernière vise à harmoniser les législations nationales dans un domaine où la libre circulation des données à caractère personnel est susceptible de porter atteinte au droit à la vie privée, et cherche à garantir un niveau élevé de protection des libertés et des droits fondamentaux à l'égard du traitement de données à caractère personnel. Les autorités de contrôle prévues à l'article 28 de la directive 95/46 sont donc les «gardiennes desdits droits et libertés fondamentaux», et leur existence est considérée «comme un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel».[23] La Cour continue comme suit (soulignement ajouté):

> «24. Pour garantir cette protection, les autorités de contrôle doivent assurer un juste équilibre entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel. Par ailleurs, en vertu de l'article 28, paragraphe 6, de la directive 95/46, les différentes autorités nationales sont appelées à coopérer entre elles et même, le cas échéant, à exercer leurs pouvoirs à la demande d'une autorité d'un autre État membre.
>
> 25. La garantie d'indépendance des autorités nationales de contrôle vise à assurer l'efficacité et la fiabilité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel et doit être interprétée à la lumière de cet objectif. Elle a été établie non afin de conférer un statut particulier à ces autorités elles-mêmes ainsi qu'à leurs agents, mais en vue de renforcer la protection des personnes et des organismes qui sont concernés par leurs décisions. Il s'ensuit que, lors de l'exercice de leurs missions, les autorités de contrôle doivent agir de manière objective et impartiale. À cet effet, elles doivent être à l'abri de toute influence extérieure, y compris celle, directe ou indirecte, de l'État ou des *Länder*, et pas seulement de l'influence des organismes contrôlés.»

Quant à l'*économie* de la directive, la Cour établit un parallèle entre la directive 95/46 d'une part, et le règlement 45/2001,[24] applicable aux institutions de l'UE et instaurant le CEPD, d'autre part. L'article 28 de la directive devrait être interprété conformément à

[19] Cour européenne de justice, arrêt, Affaire 518/07 *Commission contre République fédérale d'Allemagne*, 9 mars 2010, paragraphe 15.
[20] *Ibidem*, paragraphe 16.
[21] *Ibidem*, paragraphe 18.
[22] *Ibidem*, paragraphe 19.
[23] *Ibidem*, paragraphe 23.
[24] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physique 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* L 8/1, 12 janvier 2001.

l'article 44 du règlement exigeant que cet organe exerce ses fonctions «en toute indépendance», mais précisant aussi que le CEPD «ne sollicite ni n'accepte d'instructions de quiconque».[25] La Cour conclut ainsi que l'article 28 devrait être interprété:

> «30. […] en ce sens que les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel [...] doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure. Cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel.»

La Cour examine ensuite si la tutelle de l'État est compatible avec l'exigence d'indépendance telle que définie ci-dessus, et arrive à la conclusion que *ce n'est pas* le cas. Elle souligne également:

> «36. [...] que le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice indépendant des missions de celles-ci.»

Après une analyse approfondie, la Cour a conclu que la République fédérale d'Allemagne a manqué aux obligations qui lui incombent en vertu de l'article 28 de la directive 95/46, en soumettant à la tutelle de l'État les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel par le secteur non public dans les différents *Länder*.

Ainsi, la Cour a non seulement décidé que l'exercice des fonctions «en toute indépendance» implique de rester libre de *toute* influence extérieure, mais véhicule aussi des messages intéressants sur le rôle des autorités de contrôle: leur indépendance doit être assurée pour qu'elles puissent exercer *efficacement* leur mission, et elles devraient agir de manière *objective* et *impartiale* et assurer un *juste équilibre* entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les autres intérêts.

Nous reviendrons sur la question de savoir ce que cela pourrait signifier concernant l'interaction entre les autorités de protection des données et les institutions nationales des droits de l'homme.[26] En premier lieu, il est utile d'examiner les grandes lignes de l'actuelle révision du cadre juridique de l'UE relatif à la protection des données.

---

[25] *Ibidem*, article 44 «Indépendance»:
1. Le contrôleur européen de la protection des données exerce ses fonctions en toute indépendance.
2. Dans l'accomplissement de sa mission, le contrôleur européen de la protection des données ne sollicite ni n'accepte d'instructions de quiconque.
3. Le contrôleur européen de la protection des données s'abstient de tout acte incompatible avec le caractère de ses fonctions et, pendant la durée de celles-ci, ne peut exercer aucune autre activité professionnelle, rémunérée ou non.
4. Après la cessation de ses fonctions, le contrôleur européen de la protection des données est tenu de respecter les devoirs d'honnêteté et de délicatesse quant à l'acceptation de certaines fonctions ou de certains avantages.

[26] Voir *infra* section 6.

## 5. PROPOSITIONS CONCERNANT UN NOUVEAU CADRE JURIDIQUE DE L'UE RELATIF À LA PROTECTION DES DONNÉES

### 5.1. Motifs de la révision

Pourquoi cette révision? Pour trois grandes raisons. La *première* est la nécessité 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 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. Aujourd'hui, dans un monde où le traitement des données en continu est de plus en plus important, nous avons également besoin de garanties plus solides permettant une protection plus efficace dans la pratique. Les défis que constituent les nouvelles technologies et la mondialisation nous incitent immanquablement à faire preuve d'imagination pour proposer des innovations en vue d'une protection plus efficace.

La *deuxième* raison, c'est que le cadre actuel a renforcé la diversité et la complexité, ne fût-ce que parce qu'une directive doit, par nature, être transposée en droit national. Nous en sommes donc arrivés à 27 versions différentes de principes fondamentaux identiques. C'est tout simplement excessif, sans oublier les coûts et la perte d'efficacité que cela engendre. En d'autres termes, nous devons accélérer l'harmonisation en renforçant le système et en le rendant plus efficace dans la pratique, mais aussi plus cohérent. Ainsi, nous pourrons réduire cette diversité et cette complexité *qui ne mènent à rien*.

La *troisième* raison concerne le nouveau cadre juridique de l'UE. Le traité de Lisbonne place instamment l'accent sur les droits fondamentaux. Comme nous l'avons vu, l'article 8 de la Charte des droits fondamentaux consacre une disposition spéciale à la protection des données à caractère personnel, tandis que l'article 16 TFUE propose une nouvelle base juridique horizontale 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.

La révision du cadre vise donc à mettre en place une protection des données à caractère personnel renforcée, plus efficace, plus cohérente et plus exhaustive.

Deux propositions essentielles au moins sont à l'examen: une directive relative à l'application de la loi,[27] et un règlement directement contraignant remplaçant la directive 95/46/CE et portant sur les domaines commerciaux et le secteur public autre que les autorités chargées de l'application de la loi.[28] La directive proposée n'est pas considérée comme satisfaisante de manière générale car son niveau de protection est plus faible que celui de la proposition de règlement. Mais, dans le présent contexte, elle est également moins pertinente.

[27] 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, Bruxelles, 25 janvier 2012.

[28] 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, Bruxelles, 25 janvier 2012 (ci-après: Proposition de règlement général sur la protection des données).

### 5.2. Continuité et changement

Si nous nous penchons à présent sur le règlement proposé[29], il importe de garder présents dans notre esprit quelques messages essentiels.

Premièrement, en dépit de son caractère novateur, le règlement se caractérise par une forte continuité. Tous les concepts et principes fondamentaux actuels sont maintenus, malgré certaines clarifications et innovations.[30] L'innovation majeure consiste 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 l'exécution des droits et des obligations, pour veiller à ce que la protection soit assurée dans la pratique.

En même temps, le règlement prévoit la simplification et la réduction des coûts. La notification préalable des opérations de traitement à l'autorité de contrôle a été supprimée. Elle reste nécessaire dans les seules situations qui présentent un risque spécifique.[31] Le règlement instaure également un guichet unique pour les entreprises disposant d'établissements dans différents États membres,[32] Cela suppose l'instauration d'une autorité de contrôle centrale, à savoir, l'autorité de contrôle de l'État membre où se situe l'établissement principal de l'entreprise, qui sera la première responsable, en étroite coopération avec les autres autorités de contrôle compétentes.[33]

Un règlement directement contraignant offrira évidemment aussi une harmonisation nettement plus large - en principe: une seule règle applicable dans tous les États membres – et une plus grande cohérence. En soi, il permet également aux entreprises actives dans différents États membres de simplifier leurs obligations et de réduire fortement leurs coûts.

Enfin, la proposition de règlement a une portée générale: elle s'appliquera au secteur privé comme au secteur public. Cela est tout à fait en phase avec ce qui est prévu par la directive actuelle (directive 95/46/CE). La possibilité d'opérer une distinction systématique entre secteur public et secteur privé dans cette directive avait été explicitement examinée dans les années 90, et rejetée.

Cette approche est renforcée par l'article 8 de la Charte des droits fondamentaux, qui prévoit désormais la reconnaissance explicite du droit à la protection des données à caractère personnel, et par l'article 16 TFUE, qui 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.

### 5.3. Substance du règlement proposé

S'agissant de la substance du règlement, celui-ci renforce le rôle des partenaires-clés, à savoir les personnes concernées, les responsables du traitement des données et les autorités chargées de la protection des données. Un examen rapide des deux premiers acteurs clés permet de mieux comprendre le rôle des autorités de contrôle.

---

[29] Les références ultérieures concernent ce règlement (voir note de bas de page 28).

[30] Un exemple de l'innovation réside dans l'accent mis sur la minimisation des données, c'est-à-dire sur la nécessité de ne pas traiter plus de données que nécessaire (article 5, point c). De même, le respect de la vie privée dès la conception («privacy by design») est désormais reconnu comme un principe général (article 23).

[31] Voir l'article 34 sur la consultation préalable, par exemple lorsqu'une analyse d'impact indique un degré élevé de risques particuliers.

[32] Voir Note explicative, p. 12, paragraphe 3.4.6.2.

[33] Voir article 51, paragraphe 2.

*5.3.1. Personne concernée*

La première perspective peut également être perçue comme un renforcement du contrôle des utilisateurs: la possibilité pour les personnes concernées d'avoir une influence sur ce qu'il advient de leurs données à caractère personnel. Les droits actuels des personnes concernées ont été préservés mais surtout consolidés et étendus. Il sera également plus simple d'exercer ces droits dans la pratique.[34]

L'exigence relative au consentement a été clarifiée: *quand* il est exigé, le consentement doit être réel et solide.[35] Le droit d'objection est consolidé.[36] Les moyens mis en œuvre pour veiller au respect de ces droits dans la pratique sont également renforcés et la transparence mise en exergue.[37] Par ailleurs, une disposition introduit non pas un recours collectif à l'américaine, mais une action en nom collectif, à savoir que des organisations pourront intervenir au nom de leurs membres ou de leurs groupes constitutifs.[38]

Il est souvent question dans les débats du «droit à l'oubli» qui consiste principalement à effacer les données lorsqu'il n'existe pas de raison suffisante de les conserver.[39] De même, le droit à la portabilité des données[40] est fondamentalement une spécification du droit actuel de demander une copie de toute donnée à caractère personnel, dans un format particulier.

*5.3.2. Responsable du traitement des données*

Le principal changement concerne la considération bien plus importante portée à 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 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».[41]

Il s'agit là de l'une des principales évolutions. Cela implique aussi que la charge de la preuve incombe dans la plupart des cas à l'organisation responsable qui doit, en d'autres termes, prouver l'existence d'une base juridique adéquate, la réalité du consentement et l'efficacité continue des mesures. Cela signifie que les autorités de contrôle seront davantage impliquées dans les contrôle «ex-post», et qu'elles seront en mesure d'exiger des responsables du traitement des données des preuves suffisantes de leur conformité aux règles.

Le règlement prévoit également un certain nombre d'exigences spécifiques telles que la nécessité d'une analyse d'impact relative à la vie privée,[42] l'établissement de

[34] Articles 15 à 17
[35] Article 4, point 8, et article 7.
[36] Article 19.
[37] Article 5, point a et articles 11 et 14.
[38] Article 73, paragraphe 2, et article 76, paragraphe 1
[39] Article 17
[40] Article 18
[41] Article 22
[42] Article 33

documentation,[43] et la désignation d'un délégué à la protection des données.[44] Ces éléments sont importants pour la bonne gestion des données dans les organisations. Les délégués à la protection des données peuvent aider les organisations à respecter les dispositions et agir comme points de contact pour les autorités de contrôle.

Certaines de ces dispositions, notamment celles qui concernent la documentation, sont trop détaillées et devraient être modifiées pour être plus appropriées. Quelques exceptions figurant dans ces mêmes dispositions ne se justifient peut-être pas tout à fait. Un meilleur équilibre de cette partie de la proposition pourrait sans doute résoudre ces deux problèmes.

Une disposition générale sur la notification des violations de la sécurité est également prévue.[45] Le droit de l'Union européenne limite désormais cette notification aux seuls fournisseurs de télécommunications.

*5.3.3. Surveillance et contrôle de l'application*

Un troisième point majeur du règlement concerne le renforcement de la surveillance et du contrôle de l'application exercés par les autorités chargées de la protection de données. Les garanties prévues pour l'indépendance complète des autorités de contrôle ont été renforcées, conformément à l'arrêt de la CJUE dans l'affaire Commission/Allemagne.[46]

Le règlement confère aux autorités de contrôle des pouvoirs d'exécution renforcés dans tous les États membres, incluant à la fois des pouvoirs d'investigation, des pouvoirs d'ordonner et l'imposition de sanctions administratives.[47] Actuellement, en vertu de la directive 95/46/CE, les États membres jouissent d'une large latitude de sorte que quelques autorités de contrôle ont aujourd'hui de faibles pouvoirs et qu'aucune d'elles ne dispose de l'ensemble des pouvoirs tels qu'énoncés dans la proposition de règlement.

Les amendes administratives s'élevant à des millions d'euros (c'est-à-dire des montants équivalents à celles imposées en cas de violation du droit de la concurrence) attirent beaucoup l'attention, mais le message est le suivant: aux grands maux les grands remèdes. De cette manière, la protection des données figurera à un rang plus élevé parmi les priorités à l'ordre du jour des conseils d'administration des entreprises; pareille évolution mérite d'être saluée et pourrait se traduire par une meilleure gestion des données et une meilleure garantie des droits de la personne concernée.

La coopération internationale entre les autorités chargées de la protection des données est vivement encouragée et facilitée, y compris l'assistance mutuelle et les opérations conjointes.[48] L'instauration d'une autorité principale pour les entreprises possédant plusieurs établissements[49] est accueillie positivement, même si ladite autorité n'agira pas seule mais au sein d'un réseau, en étroite collaboration avec d'autres autorités

[43] Article 28
[44] Articles 35 à 37
[45] Articles 30 à 32
[46] Article 47
[47] Articles 53 et 79
[48] Articles 55 à 56
[49] Voir *infra* section 5.2

compétentes. Cette dimension européenne est explicitement mentionnée dans les dispositions relatives aux tâches des autorités chargées de la protection des données.[50]

Un changement très important dans cette perspective est l'instauration d'un mécanisme de contrôle de la cohérence dans le cadre du comité européen de la protection des données,[51] qui doit s'inspirer de l'actuel groupe de travail «Article 29».[52] Ce mécanisme, impliquant toutes les autorités indépendantes, garantira la cohérence des résultats de la surveillance et du contrôle de l'application dans tous les États membres. Son secrétariat sera assuré par le CEPD.[53]

*5.3.4 Protection globale de la vie privée*

Enfin, un dernier élément doit être relevé: la dimension internationale élargie du règlement, dans les deux directions. Le champ d'application du règlement a été clarifié et étendu. À présent, les dispositions s'appliqueront non seulement à tous les traitements relatifs à un établissement établi dans l'Union européenne, mais aussi aux livraisons de biens et prestations de services sur le marché européen à partir d'un pays tiers ou aux modalités de contrôle en ligne du comportement des Européens.[54]

Il s'agit d'une réalité dans le monde actuel de l'internet. En même temps, cette approche réaliste s'appuie sur une réflexion commune grandissante en matière de protection des données aux quatre coins du globe. Cela signifie que les autorités de contrôle européennes seront de plus en plus impliquées dans des problématiques de dimension internationale, y compris les pays tiers en dehors de l'UE.[55]

Une coopération internationale à plus grande échelle se développe donc actuellement entre les autorités chargées de la protection des données – 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 (GPEN). Grâce à ce réseau, il sera davantage possible de collaborer avec les acteurs mondiaux sur l'internet.[56]

[50] Voir article 46, paragraphe 1
[51] Articles 57 à 58 et 64 à 72
[52] Ce groupe de travail, instauré par l'article 29 de la directive 95/46/CE, est actif depuis 1996 et est désormais composé de représentants de toutes les DPA nationales et du CEPD. Il dispense des conseils à la Commission européenne, éventuellement à sa demande, et élabore des conseils sur des instruments non contraignants (*soft law*) concernant différents sujet, mais avec un niveau d'autorité élevé dans la pratique.
[53] Article 71
[54] Voir article 3
[55] On peut citer comme exemples récents, les enquêtes à l'encontre de Google et de Facebook menées respectivement par la CNIL et par le commissaire irlandais à la protection des données, dans lesquelles la plupart des autres DPA européennes ont été impliquées, ainsi que les autorités compétentes du Canada et des États-Unis.
[56] Cela s'explique par une convergence croissante des principes et des pratiques de protection des données dans le monde, impliquant non seulement les normes officielles élaborées par l'OCDE, le Conseil de l'Europe, l'UE, l'APEC, l'ISO et d'autres organisations, mais également d'autres instruments, tels que des codes de conduite, des règles d'entreprise contraignantes, etc.

## 6. INTERACTION ENTRE AUTORITÉS DE CONTRÔLE ET INSTITUTIONS NATIONALES DES DROITS DE L'HOMME

Que signifient toutes ces considérations pour l'interaction entre les autorités chargées de la protection des données et les institutions nationales des droits de l'homme?

Avant tout, il y a un facteur temps relativement important. Les propositions de la Commission sont actuellement en cours de discussion au Conseil et au Parlement. De toute évidence, ce n'est pas seulement une question de quelques mois et selon des estimations actuelles, des conclusions seraient attendues courant 2013, probablement sous la présidence irlandaise. Dans tous les cas, il se pourrait que le règlement proposé soit adopté d'ici 2014, moyennant certaines améliorations. En partant de cette hypothèse, le règlement pourrait entrer en vigueur en 2016. En d'autres termes, les États membres et toutes les autres parties prenantes auront le temps de se préparer à la transition. D'ici là, le cadre actuel et les législations nationales qui le mettent en œuvre, continueront d'être appliqués, sous réserve de modifications partielles, par exemple pour répondre à la jurisprudence de la CJUE.

Pour le présent, cela signifie qu'une certaine diversité continuera d'exister parmi les autorités nationales chargées de la protection des données. Or, il en va de même pour les institutions nationales des droits de l'homme. Les «Principes de Paris» examinés ailleurs dans cette publication,[57] définissent certaines normes concernant les compétences, les responsabilités, la composition et les méthodes de fonctionnement des institutions nationales, mais aucune structure, aucun mandat ni aucune forme spécifique n'est exigé. Cela signifie que l'interaction entre les autorités de contrôle et les institutions nationales des droits de l'homme peuvent avoir des modalités très variées dans les différents États membres, en fonction des conditions qui existent, y compris en termes de culture politique et de traditions.

Dans certains États membres, les autorités chargées de la protection des données, à l'instar des organismes de promotion de l'égalité de traitement et des organismes de médiation, comptent parmi les principales parties prenantes des institutions nationales des droits de l'homme et contribuent activement à leur programme, alors que ce n'est peut-être pas le cas dans d'autres États membres. Lorsqu'il existe une interaction dynamique entre les autorités de contrôle et les institutions nationales, on peut voir s'instaurer une étroite coopération dans le domaine de la sensibilisation et de l'éducation, étant donné que ces activités sont moins dépendantes des pouvoirs et procédures formels. En ce qui concerne l'inspection et le traitement des plaintes, il y a – semble-t-il – moins de chances de trouver une interaction dynamique. Toutefois, dans certains cas, les institutions nationales font un travail utile en mettant en lumière des difficultés structurelles ou des problèmes spécifiques qui pourraient faire l'objet d'une plainte ou d'une inspection, ou parfois en prenant elles-mêmes l'initiative de la plainte, d'intérêt général ou non.

À l'avenir, cela sera peut-être encore le cas, mais la principale différence sera que la grande diversité actuelle entre les autorités nationales de contrôle aura disparu ou sensiblement diminué, grâce à l'introduction par le règlement d'exigences *directement* contraignantes non seulement par rapport à l'indépendance, mais également pour les tâches et les pouvoirs des autorités de contrôle. Des règles nationales définiront probablement les détails, notamment sur la composition et la structure interne des

[57] Voir en particulier G. De Beco, «Assessment of the Paris Principles and the ICC Sub-Committee on Accreditation», chapitre 11 de ce volume.

autorités de contrôle, mais les principaux éléments seront définis dans le règlement et seront applicables directement au niveau de l'UE.

L'évolution sera perceptible: les autorités nationales chargées de la protection des données seront compétentes pour exercer leur mission dans les limites de leur propre juridiction, mais elles feront également partie intégrante d'un réseau de coopération à l'échelle de l'UE sur les questions transfrontalières et autres problématiques communes, et d'un mécanisme de contrôle de la cohérence au niveau de l'UE, visant à garantir la cohérence des résultats de la surveillance. Il est sans aucun doute un peu paradoxal de vouloir renforcer les garanties d'indépendance institutionnelle et de prendre en même temps des mesures pour réduire la diversité, inutile, entre les autorités indépendantes. L'un des principaux défis consistera bien évidemment à trouver un juste équilibre dans ce domaine. Même si des dispositions juridiques appropriées ont été fixées dans le règlement, une fois qu'il sera adopté, il s'avèrera toujours nécessaire de développer des procédures efficaces dans la pratique. Le groupe de travail «Article 29», actuelle plateforme des autorités de contrôle dans l'UE, pourrait largement contribuer à préparer le terrain à cet égard.

En ce qui concerne l'interaction avec les institutions nationales des droits de l'homme, il n'y aura probablement pas de changement majeur, hormis sans doute un environnement plus cohérent et prévisible. Dans tous les cas, l'exigence relative à l'exercice de la mission «en toute indépendance» et la nécessité d'éviter «toute influence extérieure» ne devraient pas empêcher les autorités nationales de contrôle d'établir des liens appropriés avec les institutions nationales des droits de l'homme, notamment dans le domaine général de la sensibilisation et de l'éducation, et de renforcer l'impact de ces deux activités. De fait, conformément aux Principes de Paris, des normes similaires seront applicables aux institutions nationales. Il appartiendra aux deux parties de développer et de structurer leurs relations dans leur intérêt commun.

Un élément supplémentaire doit encore être pris en considération. Si le règlement est adopté dans sa présente forme, il confèrera à «tout organisme, organisation ou association qui œuvre à la protection des droits et des intérêts des personnes concernées à l'égard de la protection de leurs données à caractère personnel» et qui a été valablement constitué conformément au droit national, «le droit d'introduire une réclamation auprès d'une autorité de contrôle dans tout État membre au nom d'une ou de plusieurs personnes concernées», s'il considère que les droits dont jouit une personne concernée en vertu du règlement ont été violés à la suite du traitement de données à caractère personnel.[58] Un droit similaire sera applicable dans le contexte des procédures juridictionnelles.[59] Cela donnera une plus grande marge de manœuvre pour les actions collectives, également dans les États membres où cette possibilité n'existe pas encore, et contribuera ainsi à une application plus efficace des règles de protection des données. Il reste à savoir dans quelle mesure cela permettra aux institutions nationales des droits de l'homme ou leurs parties prenantes de s'engager dans les questions de protection des données plus directement qu'elles ne l'ont fait jusqu'ici.

[58] Proposition de règlement général sur la protection des données, *supra* note 28, article 73.
[59] Proposition de règlement général sur la protection des données, *supra* note 28, article 76.