

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La protection des données à caractère personnel en droit européen

Van Gyseghem, Jean-Marc; de Terwangne , Cécile; Herveg, Jean; Gayrel, Claire

Published in:

Journal européen des droits de l'homme

Publication date:

2014

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Van Gyseghem, J-M, de Terwangne , C, Herveg, J & Gayrel, C 2014, 'La protection des données à caractère personnel en droit européen', *Journal européen des droits de l'homme*, numéro 1, pp. 54-87.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La protection des données à caractère personnel en droit européen¹

Data protection in European law

J.-M. Van Gyseghem, C. de Terwangne, J. Herveg et C. Gayrel

Résumé

Cette chronique dédiée à la vie privée, et principalement à la protection des données, sera divisée en deux parties. La première présentera la situation législative au niveau de l'Union européenne et du Conseil de l'Europe tandis que la seconde donnera une vue d'ensemble de la jurisprudence liée à ces législations.

Cette approche nous apparaît pertinente afin de pouvoir aborder la matière de la protection des données à caractère personnel qui est assez complexe et méconnue.

Pour ce qui concerne la jurisprudence, nous présentons les décisions récentes même si certaines, plus anciennes, sont également évoquées car toujours citées par les Cours européennes.

Abstract

This column dedicated to privacy, and mainly data protection, will be divided in two parts. Part I presents the state of European legislation (European Union and Council of Europe) as it is today. Part II will give an overview of the case-law implementing the regulatory framework.

This two-steps approach seems to us appropriate to introduce to an area – the protection of personal data – that is highly complex and often poorly understood.

As regards the case-law, the focus is on the most recent decisions, although some earlier cases are also mentioned insofar as they are cited as precedent and relied on by the European courts.

Introduction

La présente chronique dédiée à la protection de la vie privée et des données à caractère personnel étant la première dans le cadre du *Journal européen des droits de l'homme*, il est apparu opportun de la subdiviser en deux parties, à savoir une chronique législative et une chronique de jurisprudence. Cela permettra, dans un premier temps, de rappeler la législation européenne tant au niveau du Conseil de l'Europe que de l'Union européenne et, dans un second temps, d'y raccrocher la jurisprudence qui nous paraît pertinente sans prétendre à l'exhaustivité.

¹ Voir également : E. DEGRAVE, C. GAYREL, J. HERVEG, S. HALLEMANS, Q. VAN ENIS, J.-M. VAN GYSEGHEN et M. VAN WINCKEL, « Libertés et société de l'information », *R.D.T.I.*, 2012, pp. 68-127.

Cette double approche semble la plus pertinente pour aborder la matière complexe et méconnue qu'est la protection des données à caractère personnel.

En termes de jurisprudence, les commentaires qui suivent sont centrés sur les décisions récentes pour chaque thème abordé. Cependant, certaines décisions sont plus anciennes mais méritent d'être relevées car leur pertinence est avérée dès lors qu'elles servent encore de référence dans des arrêts récents.

I. État de la législation

A. CONSEIL DE L'EUROPE

Article 8 de la Convention européenne des droits de l'homme. L'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH, ci-après) concerne la protection de la vie privée et familiale et énonce ce qui suit :

■ « 1 Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2 Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est *prévues 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 »². ■

Rédigée telle quelle en 1950, cette disposition fera l'objet d'une interprétation « dynamique » de la part de la Cour européenne des droits de l'homme qui permettra de faire découler du droit au respect de la vie privée des éléments de la protection des données à caractère personnel.

Convention 108. La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée le 28 janvier 1981, est, à l'heure actuelle, le seul standard à la fois international et juridiquement contraignant en matière de protection des données. La Convention est en effet également ouverte aux États non membres du Conseil de l'Europe. En 2013, l'Uruguay a ainsi été le premier pays non européen à y adhérer.

La Convention 108 n'a, en principe, pas d'effet direct au sein des ordres juridiques de ses États parties. Toutefois, la question de l'effet direct des conventions internationales est en dernier ressort tranchée par le droit national de l'État considéré.

² Nous soulignons.

Dans certains États³, certaines dispositions de la Convention se sont vues reconnaître un effet direct, faisant de la Convention une pierre angulaire du système national de protection des données.

Cette Convention contient en effet les principes de base de la protection des données. Ces principes ont été repris dans la plupart des textes nationaux et internationaux en la matière et sont toujours d'actualité aujourd'hui, même s'ils nécessitent sans doute certains compléments. Ces principes sont les suivants :

- principe de loyauté et licéité de la collecte des données ;
- principe de finalité (les données sont enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités) ;
- principe de qualité des données (pertinentes, adéquates, à jour et conservées pour une durée limitée en fonction de la finalité poursuivie) ;
- régime spécifique réservé aux données sensibles ;
- exigence de sécurité ;
- droits d'accès, de rectification et de recours octroyés à la personne concernée par les données ;
- possibilité de dérogations au nom d'intérêts publics ou privés prépondérants.

À l'approche des trente ans de sa Convention 108, le Conseil de l'Europe a entamé un travail de modernisation de ce texte afin de le mettre en phase avec les évolutions technologiques majeures apparues depuis sa naissance en 1981⁴.

Il faut savoir que la Convention a déjà été complétée en 2001 par un Protocole additionnel⁶. Ce dernier a eu pour but de renforcer la mise en œuvre des principes contenus dans la Convention par l'ajout de deux nouvelles dispositions dont l'une traite des autorités de contrôle spécifiques à mettre en place par chaque partie, tandis que l'autre règle le sort des flux transfrontières de données à caractère personnel vers les pays non parties à la Convention. Ces deux compléments n'apportent certes pas à eux seuls la réponse aux nouveaux défis qui se sont fait jour.

Les définitions et principes fixés par la Convention 108 ont permis tant aux juridictions nationales qu'à la Cour européenne des droits de l'homme d'assurer une protection des individus face à l'expansion des flux d'information les concernant.

³ Tel Andorre par exemple.

⁴ Les textes issus des travaux de modernisation menés au Conseil de l'Europe sont mis à disposition du public sur le site Internet de l'institution. Voy. le document reprenant les propositions de modernisation de la Convention 108 (T-PD_2012_04_rev4_fr) adopté par le Comité consultatif de la Convention le 30 novembre 2012, http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/TPD_2012_04_rev_fr.pdf.

⁵ Pour d'amples développements sur ces éléments de modernisation du texte, voy. C. DE TERWANGNE et J.-Ph. MOINY, « La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et les concepts fondamentaux de la protection des données », in C. DE TERWANGNE (éd.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, chap. 2.2., pp. 48 à 98.

⁶ 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, signé à Strasbourg le 8 novembre 2001.

Résolutions et recommandations. De manière complémentaire à l'article 8 CEDH et la Convention 108, il est utile de relever que le Conseil de l'Europe a adopté une série de résolutions et recommandations dans des matières particulières sur lesquelles un consensus a pu être atteint au niveau européen. C'est à ce titre que ces textes présentent un intérêt à défaut d'avoir une force juridique contraignante. Il est également intéressant de relever que ces résolutions et recommandations inspirent la Cour européenne des droits de l'homme dans sa recherche du consensus européen sur certaines valeurs ou certains équilibres à respecter. Elles peuvent servir également aux cours et tribunaux nationaux appelés à se pencher sur des questions évoquées par ces textes. C'est par exemple dans un de ces textes que l'on trouve la seule définition « institutionnelle » de la vie privée ou une définition du profilage. Les paragraphes qui suivent présentent brièvement les résolutions et recommandations traitant de questions liées à la protection de la vie privée et des données à caractère personnel.

Résolution 1165 (1998). En 1998, l'Assemblée parlementaire du Conseil de l'Europe a adopté une résolution sur le droit au respect de la vie privée complétant la Déclaration 428 de 1970 qui avait défini le droit au respect de la vie privée comme étant « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence »⁷. Près de trente ans plus tard, l'Assemblée a précisé que « pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition le droit de contrôler ses propres données »⁸.

Recommandation CM/Rec(2012)4⁹. Les Résolutions et Recommandations ayant cette aptitude – et, peut-être, est-ce leur utilité première – de coller le plus possible à l'actualité, l'Assemblée parlementaire a adopté une Recommandation sur la protection des droits de l'homme dans le contexte des services de réseaux sociaux en 2012. Si elle relève le rôle majeur des réseaux sociaux dans l'exercice et la jouissance par les individus de leurs droits et libertés fondamentales, elle ne manque pas de souligner les menaces suscitées par ces réseaux pour le droit au respect de la vie privée et de la dignité humaine. Face à ces menaces identifiées, le texte recommande aux fournisseurs de ces réseaux de notamment informer clairement les utilisateurs, en leur offrant des outils accessibles, de leur droit de limiter l'accès à leurs données, ainsi que le droit de supprimer celles-ci des archives et des fichiers temporaires des moteurs de recherche. Les utilisateurs devraient toujours avoir la possibilité de clôturer leur compte et de transférer vers un autre service, aisément et dans un format exploitable, les données et images qu'ils ont enregistrées. Une fois un compte personnel clôturé, toutes les données relatives à

⁷ Résolution de l'Assemblée parlementaire du Conseil de l'Europe 428 (1970) portant déclaration sur les moyens de communication de masse et les droits de l'homme, assembly.coe.int/mainf.asp?Link=/documents/adoptedtext/ta70/fres428.htm.

⁸ Résolution de l'Assemblée parlementaire du Conseil de l'Europe 1165 (1998) sur le droit à la vie privée, C.2., assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta98/FRES1165.htm, point 5.

⁹ Recommandation CM/Rec(2012)4 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, wcd.coe.int/ViewDoc.jsp?id=1929465&Site=CM.

l'utilisateur de ce compte devraient être définitivement supprimées de la zone de stockage du service de réseau social.

Lorsque des applications tierces sont autorisées à accéder aux données à caractère personnel des utilisateurs enregistrées au sein du réseau social, ce dernier devrait proposer des catégories d'accès de plusieurs niveaux de sorte que les utilisateurs puissent consentir à l'accès à certaines catégories de données et pas à d'autres.

Le droit d'utiliser un pseudonyme devrait être garanti en tant que condition du plein exercice de la liberté d'expression et du droit de communiquer et de recevoir des informations, de même que de la pleine jouissance du droit au respect de la vie privée. «Lorsqu'un service de réseau social exige une identité réelle pour s'enregistrer sur son site, la diffusion de l'identité des utilisateurs sur internet devrait être facultative»¹⁰.

Recommandation CM/Rec(2012)3¹¹. Une autre Recommandation adoptée le même jour par le Conseil des Ministres et portant sur la protection des droits de l'homme dans le contexte des moteurs de recherche, relève que l'activité des moteurs de recherche peut menacer les droits de l'homme et les libertés fondamentales, spécialement la liberté d'expression, la liberté d'accès à l'information, le droit au respect de la vie privée et à la protection des données à caractère personnel.

Ainsi, les moteurs de recherche traitent d'impressionnantes quantités de données à caractère personnel qui révèlent le comportement de recherche des individus. L'historique des recherches effectuées par une personne sur un moteur de recherche est remarquablement révélateur de ses centres d'intérêt, de ses projets, de ses intentions, de ses préférences. Il peut aussi dévoiler des données sensibles (c'est-à-dire des données révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ou des données relatives à la santé, à la vie sexuelle ou à des condamnations pénales). En conséquence, il est recommandé aux États une série de mesures parmi lesquelles veiller à ce que la collecte de données à caractère personnel par les fournisseurs de moteurs de recherche soit minimisée, veiller à ce que la durée de conservation ne soit pas plus longue que ce qui est strictement nécessaire aux finalités légitimes et spécifiées du traitement. Les fournisseurs de moteurs de recherche devraient fournir des informations sur la durée de conservation qui soient publiques et facilement accessibles, etc.

¹⁰ Annexe à la Recommandation CM/Rec(2012)4, § 3. «Cela n'empêche pas pour autant les autorités chargées de l'application de la loi d'avoir accès à la véritable identité d'un internaute lorsque cela s'avère nécessaire et sous réserve de conformité aux garanties juridiques appropriées garantissant le respect des droits et des libertés fondamentales» (*ibid.*).

¹¹ Recommandation CM/Rec(2012)3 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, wcd.coe.int/ViewDoc.jsp?id=1929441&Site=CM.

Les moteurs de recherche devraient en outre répondre rapidement aux demandes d'utilisateurs d'effacer leurs données à caractère personnel à partir (d'extraits) des copies des pages web que les fournisseurs de moteurs de recherche stockent encore éventuellement (dans leur « cache ») une fois le contenu original effacé.

Résolution 1843 (2011)¹². Cette résolution 1843 (2011)¹ de l'Assemblée parlementaire sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne contient des principes généraux concernant la protection de la vie privée et des données à caractère personnel dans un environnement de TIC. Au titre du premier de ces principes, l'Assemblée proclame que « la protection de la vie privée est un élément nécessaire de la vie humaine et du fonctionnement humain d'une société démocratique ; toute violation de la vie privée d'une personne met en jeu sa dignité, sa liberté et sa sécurité ».

Ensuite le texte érige en droit fondamental le droit à la protection de la vie privée et des données à caractère personnel. Ce droit implique pour chacun le droit de contrôle de l'utilisation des données le concernant.

La résolution détaille encore différents principes parmi lesquels la protection accrue à accorder aux images privées et aux données à caractère personnel des mineurs ou des personnes souffrant d'un handicap mental ou psychologique, et le principe de limitation « au plus strict minimum » du volume des données à caractère personnel traitées.

Recommandation (2010)13¹³. Adoptée le 23 novembre 2010, cette recommandation du Comité des Ministres du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage suggère un encadrement du phénomène très répandu du profilage. Ce dernier est défini comme étant « une technique de traitement automatisé des données qui consiste à appliquer un “profil” à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels ». Le « profil » devant quant à lui s'entendre d'un « ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu ».

L'annexe à la recommandation contient les principes devant conduire à un profilage loyal et licite. Une liste des cas dans lesquels le profilage est licite est établie. Le responsable est tenu de limiter les risques d'erreurs, d'adopter des mesures de sécurité et d'informer les personnes concernées de ses activités de profilage. Sauf exceptions, les individus ont le droit d'accéder aux données, de les corriger, de connaître le but du profilage ainsi que la logique utilisée pour leur attribuer un

¹² Résolution 1843 (2011)¹ relative à la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne, assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/FRES1843.htm.

¹³ Recommandation du Comité des Ministres du Conseil de l'Europe (2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, wcd.coe.int/ViewDoc.jsp?id=1710937&Site=CM.

profil, et enfin, de s'opposer à l'utilisation de leurs données ou à une décision prise sur la seule base du profilage.

Recommandation (99)5¹⁴. Cette recommandation du Comité des Ministres du Conseil de l'Europe du 23 février 1999 sur la protection de la vie privée sur Internet s'adresse aux utilisateurs et aux fournisseurs de services sur Internet. Elle contient des lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes », destinées à être intégrées dans des codes de conduite. Ces lignes directrices énoncent les principes d'une conduite loyale à observer en matière de protection de la vie privée et des données lors des communications et échanges sur Internet.

B. UNION EUROPÉENNE

Charte des droits fondamentaux de l'Union européenne. Depuis l'entrée en vigueur du Traité de Lisbonne, la Charte des droits fondamentaux de l'Union européenne¹⁵ est juridiquement contraignante. Ce texte est particulièrement intéressant car il présente la spécificité, par rapport aux traités de protection des libertés fondamentales classiques, de garantir, outre la protection de la vie privée, la protection des données à caractère personnel en un article 8 inédit. Cet article élève ainsi la protection des données à caractère personnel au rang de droit fondamental *in se* même s'il garde cette particularité de rester lié à d'autres droits et libertés tels que la liberté d'association, le droit à la vie privée et la liberté d'expression.

Cet article 8 dispose donc que :

- « 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 »¹⁶.

Il est intéressant de constater que la note du Presidium¹⁷ rattache ce droit tant à l'article 8 CEDH qu'à la Convention du Conseil de l'Europe pour la protection des

¹⁴ Recommandation du Comité des Ministres du Conseil de l'Europe (99)5 du 23 février 1999 sur la protection de la vie privée sur Internet, wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276586&SecMode=1&DocId=396770&Usage=2.

¹⁵ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:FR:PDF>.

¹⁶ http://www.europarl.europa.eu/charter/pdf/text_fr.pdf.

¹⁷ http://www.europarl.europa.eu/charter/pdf/04473_fr.pdf.

personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ratifiée par tous les États membres, qu'à encore, la directive 95/46/CE du Parlement européen et du Conseil 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 dont il sera question ci-dessous.

Cette filiation entre ces divers textes de base en matière de protection des données à caractère personnel est établie afin de renforcer l'encrage de ce nouveau droit dans le droit européen d'autant plus que, en vertu de l'article 52.3 de la Charte¹⁸, le sens du droit à la protection des données à caractère personnel ainsi que sa portée sont les mêmes que ceux conférés par la CEDH.

Cet article 8 de la Charte doit également être lu en parallèle avec l'article 6 du Traité de l'Union qui prescrit que :

■ « 1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités.

Les dispositions de la Charte n'étendent en aucune manière les compétences de l'Union telles que définies dans les traités.

(...)

3. Les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux». ■

Pour ce qui est de l'exercice de ce droit et, notamment, des limitations possibles, la note du Presidium renvoie à la directive 95/46 et à l'article 52 de la Charte.

Directive européenne 95/46. La directive 95/46 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 données¹⁹ a repris, en les détaillant et les précisant, les principes contenus dans la Convention 108 du Conseil de l'Europe. Elle présente toutefois un régime de protection enrichi sur plus d'un point.

¹⁸ « Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ».

¹⁹ 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, *J.O.C.E.*, 23 novembre 1995, n° L 281, pp. 31-50. Voy. M.-H. BOULANGER, C. DE TERWANGNE, T. LEONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, « La protection des données à caractère personnel en droit communautaire, *J.T. dr. eur.*, 1997, pp. 121 et s.

Étant donné que cette directive a fait l'objet d'une transposition en droit belge, l'ensemble de ses dispositions se retrouvent dans la loi du 8 décembre 1992 telle que modifiée en 1998. La directive accordait 3 ans aux États membres pour mettre leur législation en conformité avec ses prescrits²⁰.

On relèvera les innovations majeures apportées par le texte européen :

- La directive a établi une liste des seuls cas dans lesquels le traitement des données est *a priori* légitime²¹.
- Le catalogue des droits reconnus à la personne concernée est particulièrement étoffé. Le droit d'accès dépasse le simple droit d'avoir connaissance des données faisant l'objet d'un traitement, et englobe désormais le droit de connaître l'origine des données et la logique qui sous-tend le traitement des données²². Le droit de s'opposer au traitement de ses données²³ et le droit de ne pas être soumis à une décision individuelle entièrement automatisée²⁴ sont consacrés.
- En outre, un devoir d'information est mis à charge du responsable du traitement des données²⁵.
- Enfin, le régime des flux transfrontières de données qui a, lui, par la suite, inspiré le Protocole additionnel à la Convention 108, est particulièrement élaboré.

Cette directive 95/46 a tenté, sans malheureusement y parvenir entièrement, de donner à l'Union européenne un régime uniforme en matière de protection des données à caractère personnel.

Il est à noter que cette directive est en pleine mutation dès lors que la Commission européenne a lancé un processus de révision qui devrait aboutir à la transformation du texte en règlement européen²⁶. Cependant, les modifications proposées suscitent d'intenses réflexions et des réactions singulièrement nombreuses, ce qui a empêché le processus de révision d'aboutir à l'heure actuelle.

Directive européenne vie privée et communications électroniques²⁷. La directive 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques²⁸ est une directive spécifique qui vient compléter la

²⁰ La Belgique n'eut en apparence que quelques semaines de retard sur ce délai puisque c'est le 11 décembre 1998 qu'elle votait la loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel mais cette loi n'est, en fait, entrée en vigueur que le 1^{er} septembre 2001. En outre, pour de nombreuses dispositions, un arrêté d'exécution était nécessaire. Cet arrêté a été adopté le 13 février 2001 mais n'est également entré en vigueur que le 1^{er} septembre 2001.

²¹ Article 7 de la directive 95/46.

²² Article 12 de la directive 95/46.

²³ Article 14 de la directive 95/46.

²⁴ Article 15 de la directive 95/46.

²⁵ Articles 10 et 11 de la directive 95/46.

²⁶ Voy. C. GAYREL et R. ROBERT, « Proposition de règlement sur la protection des données – Premiers commentaires », *J.D.E.*, 2012, pp. 173 à 181.

²⁷ Cette directive a été transposée en Belgique par la loi du 13 juin 2005 relative aux communications électroniques.

²⁸ *J.O.U.E.*, L 201 du 31 juillet 2002, pp. 37-47.

directive générale (95/46) pour réglementer la protection des données dans le secteur spécifique des communications électroniques. Cette directive fait partie du «paquet télécom».

Cette directive 2002/58 ne s'applique qu'aux fournisseurs de services de communications électroniques accessibles au public, ce qui peut, dans certains domaines, générer des distorsions de concurrence au bénéfice d'opérateur ne fournissant pas de tels services de communications électroniques accessibles au public mais offrant cependant des services à valeur ajoutée basés sur la localisation tels que ceux que l'on trouve sur les GPS de voiture. Ce texte règle aussi le recours aux cookies et l'envoi de communications non sollicitées (spam).

Cette directive traite de la confidentialité des communications de manière telle que les États membres doivent garantir, «par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes»²⁹. Cette confidentialité doit être garantie à l'égard de tout tiers à une communication électronique de manière telle que les États membres interdisent à toute autre personne que les utilisateurs parties à la communication électronique «d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs [parties à la communication électronique] sauf lorsque cette personne y est légalement autorisée»³⁰. Bien entendu, «le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité»³¹ n'est pas empêché par cette interdiction.

Par ailleurs, le stockage «des informations ou [l'accès] à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur [ne sont permis] qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données»³². La directive met donc en exergue l'information de l'abonné ou de l'utilisateur et son droit de refus.

De plus et sauf exception, «les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication» sous réserve d'exceptions prévues par les États membres ou par la directive elle-même³³. À noter que, parmi ces

²⁹ Directive 2002/58/CE, article 5.

³⁰ Directive 2002/58/CE, article 5.1.

³¹ Directive 2002/58, article 5.1, *in fine*.

³² Directive 2002/58, article 5.2.

³³ Directive 2002/58, article 6.1.

exceptions, nous retrouvons l'activité commerciale du fournisseur de services qui lui permet de traiter ces données relatives au trafic « pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement »³⁴, consentement qui peut être retiré à tout moment.

La directive traite également des données de localisation autres que les données relatives au trafic en prescrivant que leur traitement ne pourra être effectué « qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée »³⁵. Le consentement devra, bien entendu, être éclairé, ce qui implique une information quant « au type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée »³⁶. Par ailleurs et en cas de consentement, les utilisateurs ou les abonnés « doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication »³⁷.

Directive européenne «data retention»³⁸. La directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications a modifié la directive 2002/58/CE analysée ci-dessus mais fait l'objet d'une procédure de réflexion initiée par la Commission européenne sur l'opportunité de modifier cette directive suite aux refus de plusieurs États membres de la transposer ou à des décisions de Cours constitutionnelles annulant les lois de transposition pour inconstitutionnalité³⁹. Cette directive continue en effet à faire débat par rapport à sa légalité dans nombre d'États membres. Elle soulève nombre de questions par rapport à certains principes clés en matière de protection de la vie privée tel que celui de nécessité prévu par l'article 8 CEDH.

Le principe de cette directive qui s'inscrit dans la mouvance des textes pris dans un contexte de lutte contre le terrorisme et la criminalité organisée est d'obliger les fournisseurs de services de communications électroniques accessibles au public à conserver une série de données pour une durée allant de 6 mois à 2 ans.

³⁴ Directive 2002/58, article 6.3.

³⁵ Directive 2002/58, article 9.1.

³⁶ Directive 2002/58, article 9.1.

³⁷ Directive 2002/58, article 9.2.

³⁸ La Belgique a transposé cette directive par la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90^{decies} du Code d'instruction criminelle. Ainsi, les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic pour l'accomplissement de certaines procédures précisées par la loi. La loi précise également, en son article 5, que « sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée ».

³⁹ Voy., entre autres, K. DE VRIES, R. BELLANOVA et P. DE HERT, « Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention », Centre for European Policy Studies, mai 2010.

Ces données sont précisées à l'article 5 de cette directive et consistent, par exemple, dans le numéro d'appel de l'appelant, le numéro IMEI de l'appelé, etc.

Règlement 45/2001 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 de la Communauté et la libre circulation de ces données. Ce règlement est très similaire à la directive 95/46 vue ci-dessus à la différence près qu'il vise exclusivement la protection des données à caractère personnel traitées par les institutions et organes de l'Union européenne, en ce compris les agences.

Outre qu'il a mis en place des principes de protection des données à caractère personnel identiques à ceux de la directive 95/46, le Règlement a institué un Contrôleur européen à la protection des données (CEPD) dont le rôle est similaire à celui des autorités de contrôle nationales avec un accès direct pour les citoyens. Des délégués à la protection des données doivent en outre être désignés par chaque institution ou organe de l'Union européenne.

II. État de la jurisprudence

A. COUR EUROPÉENNE DES DROITS DE L'HOMME

Notion de vie privée. La Cour européenne des droits de l'homme a eu l'occasion de préciser l'étendue de la notion de « vie privée » protégée par l'article 8 CEDH :

■ « La “vie privée” est une notion large, qui ne se prête pas à une définition exhaustive. (...). Elle peut s'étendre à des activités professionnelles ou commerciales. Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la “vie privée” »⁴⁰. ■

En 2012, elle a également rappelé que « la publication d'une photo interfère dès lors avec la vie privée d'une personne, même si cette personne est une personne publique »⁴¹ et que « dans certaines circonstances, une personne, même connue du public, peut se prévaloir d'une “espérance légitime” de protection et de respect de sa vie privée »⁴². L'on doit cependant relever que, dans le cadre de cet arrêt qui concernait Caroline de Monaco, la Cour a estimé que les juridictions allemandes avaient modifié leur jurisprudence antérieure suite à l'arrêt de la Cour de 2004 condamnant l'Allemagne (*cf. infra*) et n'a pas fait droit à la requête au motif que les photos documentaient un article concernant la maladie du Prince Rainier qualifiée d'« événement de l'histoire contemporaine » et donc justifiant leur publication.

⁴⁰ Cour eur. D.H., *Peck c. Royaume-Unis*, 28 janvier 2003, req. n° 44647/98, § 57 ; nous soulignons.

⁴¹ Cour eur. D.H., *von Hannover c. Allemagne*, 7 février 2012, req. n°s 40660/08 et 60641/08, § 95.

⁴² Cour eur. D.H., *von Hannover c. Allemagne*, 7 février 2012, req. n°s 40660/08 et 60641/08, § 97.

Des informations publiques peuvent relever de la vie privée quand elles sont systématiquement collectées et enregistrées dans des fichiers tenus par les autorités⁴³ et ce même lorsque les informations concernent le passé lointain d'une personne⁴⁴. La Cour a noté que cette interprétation correspondait à la notion de vie privée développée dans la Convention du 28 janvier 1981 du Conseil de l'Europe. Le fait de conserver et de communiquer à une juridiction un rapport de police inexact constitue une ingérence dans le droit au respect de la vie privée⁴⁵.

Admissibilité des ingérences. Si le principe de l'article 8 consacre le droit à la vie privée et familiale dans le chef de l'individu, il fixe également des exceptions à ce droit au paragraphe 2, paragraphe qui « appelle une interprétation étroite »⁴⁶. Cependant, ces exceptions ne sont admises qu'aux conditions de légalité, de légitimité et de nécessité.

Le principe de nécessité ou de proportionnalité impose à chaque État souhaitant limiter le droit à la vie privée de procéder à une analyse de proportionnalité entre, d'une part, la protection de la vie privée et, d'autre part, les intérêts publics ou privés méritant également une protection. Il s'agit de la pierre angulaire du régime des exceptions de l'article 8 de la Convention. La Cour européenne des droits de l'homme a cependant considéré « qu'il convenait d'accorder aux autorités nationales compétentes une certaine latitude pour établir un juste équilibre entre les intérêts publics et privés qui se trouvent en concurrence. Cependant, cette marge d'appréciation va de pair avec un contrôle européen (*Funke c. France*, arrêt du 25 février 1993, série A n° 256-A, p. 24, § 55) et son ampleur est fonction de facteurs tels que *la nature et l'importance des intérêts en jeu et la gravité de l'ingérence* (*Z c. Finlande*, arrêt du 25 février 1997, *Rec.* 1997-I, p. 348, § 99) »⁴⁷.

La Cour a, par ailleurs, rappelé l'obligation en vertu de laquelle l'exception/l'ingérence doit être prévue par la loi. « Les mots "prévues par la loi" imposent non seulement que la mesure incriminée ait une base en droit interne, mais visent aussi la qualité de la loi en cause : ainsi, celle-ci doit être accessible au justiciable et prévisible »⁴⁸. Cela « implique ainsi – et cela ressort de l'objet et du but de l'article 8 – que le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par le paragraphe 1 (...). Or le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret (...) »⁴⁹.

Si les concepts de « base en droit interne » et d'accessibilité ne posent pas de problème au niveau de leur compréhension, la Cour a estimé nécessaire de préciser

⁴³ Cour eur. D.H., *Antunes Rocha c. Portugal*, 31 mai 2005, req. n° 64330/01 ; Cour eur. D.H., *Segerstedt-Wiberg And Others c. Sweden*, 6 juin 2006, req. n° 62332/00.

⁴⁴ Cour eur. D.H., *Cemalettin Canli c. Turquie*, 18 novembre 2008, req. n° 22427/04.

⁴⁵ Cour eur. D.H., *Cemalettin Canli c. Turquie*, 18 novembre 2008, req. n° 22427/04.

⁴⁶ Cour eur. D.H., *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, § 47.

⁴⁷ Cour eur. D.H., *Peck c. Royaume-Uni*, 28 janvier 2003, req. n° 44647/98, § 77 ; nous soulignons.

⁴⁸ Cour eur. D.H., *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, § 52.

⁴⁹ Cour eur. D.H., *Amann c. Suisse*, 16 février 2000, req. n° 27798/95, § 56.

« qu’une norme est “prévisible” lorsqu’elle est rédigée avec assez de précision pour permettre à toute personne, en s’entourant au besoin de conseils éclairés, de régler sa conduite⁵⁰. La loi doit donc fixer, entre autres, le genre d’informations pouvant être traitées, les catégories de personnes auprès desquelles les données peuvent être collectées et les circonstances précises dans lesquelles les données peuvent être collectées. Cela permettra ainsi à l’individu de vérifier la compatibilité de la loi avec la prééminence du droit ainsi qu’un contrôle *a posteriori* de la bonne mise en œuvre de la loi.

Passage de la protection de la vie privée à la protection des données à caractère personnel. Le lien entre la protection de la vie privée et la protection des données à caractère personnel a été opérée par la Cour européenne des droits de l’homme, entre autres, dans un arrêt du 4 décembre 2008 dans lequel elle précise que :

■ « La protection des données à caractère personnel joue un rôle fondamental pour l’exercice du droit au respect de la vie privée et familiale consacré par l’article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (voir, *mutatis mutandis*, *Z c. Finlande*, précité, § 95) »⁵¹. ■

La Cour a fortement insisté sur le fait que la protection des données à caractère personnel (les informations relatives à la santé n’en étant pas les moindres) joue un rôle fondamental pour l’exercice du droit au respect de la vie privée et familiale, étant donné que le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique des États membres. Par voie de conséquence, la législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l’article 8⁵². Ce principe (dont il n’était pas évident de soutenir qu’il ne concernait pas que les données médicales) a ensuite été affirmé de manière explicite pour toutes les données à caractère personnel⁵³. La nécessité de disposer de telles garanties se fait d’autant plus sentir lorsqu’il s’agit de protéger des données soumises à un traitement automatique, en particulier lorsqu’elles sont utilisées à des fins policières⁵⁴.

Sécurité et confidentialité. Dans l’affaire *Panteleyenko*⁵⁵, une juridiction ukrainienne avait demandé et obtenu d’un hôpital psychiatrique des informa-

⁵⁰ Cour eur. D.H., *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, § 55.

⁵¹ Cour eur. D.H., *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n°s 30562/04 et 30566/04, § 103.

⁵² Cour eur. D.H., *LL c. France*, 10 octobre 2006, req. n° 7508/02. Ceci a été répété dans l’arrêt du 17 juillet 2008, *I. c. Finlande*, req. n° 20511/03, ainsi que dans l’arrêt du 25 novembre 2008, *Biriuk c. Lituanie*, req. n° 23373/03, ce dernier arrêt concernant la publication d’un article sur l’état de santé de la requérante qui contenait également des références sur sa vie sexuelle.

⁵³ Cour eur. D.H., *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n°s 30562/04 et 30566/04.

⁵⁴ Cour eur. D.H., *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n°s 30562/04 et 30566/04.

⁵⁵ Cour eur. D.H., *Panteleyenko c. Ukraine*, 29 juin 2006, req. n° 11901/02.

tions confidentielles concernant l'état de la santé mentale du requérant ainsi que son traitement médical. Ces informations avaient ensuite été divulguées par le tribunal aux parties et aux autres personnes présentes. La Cour a rappelé qu'il s'agissait d'une ingérence par une autorité publique et que celle-ci était injustifiée dès lors que le tribunal n'avait pas respecté les règles applicables aux traitements de données psychiatriques qui, de plus, n'étaient en rien utiles pour la solution du litige⁵⁶. Dans le même ordre d'idées, dans l'affaire *LL c. France* à propos de l'admissibilité et de l'utilisation par un juge d'une pièce médicale en tant qu'élément de preuve dans une procédure en divorce, la Cour a indiqué que l'ingérence qui découle inévitablement de ce type de preuve doit se limiter aux pièces rendues strictement nécessaires par les spécificités de la procédure, d'une part, et par les données du litige, d'autre part. En l'espèce, c'était de façon subsidiaire et surabondante que les juridictions internes avaient invoqué la pièce médicale litigieuse pour fonder leurs décisions. Elles auraient donc pu l'écarter tout en parvenant à la même conclusion. L'ingérence n'était dès lors pas proportionnée au but recherché et n'était pas nécessaire dans une société démocratique à la protection des droits et libertés d'autrui.

La Cour a été saisie du cas d'une infirmière qui avait vu son contrat de travail non renouvelé après que des rumeurs eurent circulé sur son état de santé. Celle-ci avait échoué à obtenir réparation de son préjudice devant les juridictions finlandaises qui considéraient qu'elle ne rapportait pas la preuve de l'accès non autorisé à son dossier médical tenu dans l'hôpital où elle travaillait. La Cour a considéré qu'il était excessif de mettre à charge de la requérante la preuve d'une relation causale entre les manquements dans les règles de sécurité d'accès et la divulgation de données médicales, alors que ces manquements étaient établis. Elle a noté qu'il était évident que si l'hôpital avait mieux protégé l'accès aux dossiers médicaux en restreignant leur accès aux professionnels de la santé directement impliqués dans le traitement de la requérante ou en conservant un registre de toutes les personnes qui avaient eu accès au dossier médical de la requérante, celle-ci aurait été mise dans une situation moins défavorable devant les juridictions internes dans son action en responsabilité. À cet égard, la possibilité d'obtenir une indemnisation pour le dommage causé par une divulgation non autorisée de données à caractère personnel n'est pas suffisante pour protéger la vie privée. Ce qui est requis en premier est une protection réelle et effective qui exclut toute possibilité d'accès non autorisé⁵⁷. Voici les États membres, les hôpitaux et les praticiens de la santé prévenus...

⁵⁶ Cour eur. D.H., *LL c. France*, 10 octobre 2006, req. n° 7508/02. De plus, la cour a considéré que le droit français n'offrait pas de garanties suffisantes lors de l'utilisation de données relevant de la vie privée des parties dans ce type de procédure ce qui justifie à plus forte raison un strict contrôle de la nécessité de ces ingérences (voy. un cas comparable mais qui a donné lieu à une décision contraire : arrêt *N.N. et T.A. c. Belgique* du 13 mai 2008, req. n° 65097/01).

⁵⁷ Cour eur. D.H., *I. c. Finlande*, 17 juillet 2008, req. n° 20511/03. Voy. sur cette question C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 7 mai 2009, *R.D.T.I.*, 2011, n° 43, pp. 65-81.

Prise de photographies. L'image d'un individu est un des attributs principaux de sa personnalité du fait qu'elle dégage son originalité et lui permet de se différencier de ses congénères. Le droit de l'individu à la protection de son image constitue ainsi un des composants essentiels de son épanouissement personnel et présuppose principalement la maîtrise de celle-ci par lui. Si la maîtrise de son image implique, dans la plupart des cas, la possibilité, pour l'individu, de refuser la diffusion de son image, elle comprend, en même temps, le droit de s'opposer à la captation, la conservation et la reproduction de celle-ci par autrui. Le fait que l'individu soit une personne publique ou un personnage d'actualité peut justifier, dans certaines circonstances, la captation de son image à son insu et sans son consentement, en vue de servir l'intérêt général⁵⁸.

Dans le cadre d'une prise en charge hospitalière où des abus sexuels étaient suspectés à charge d'un père mais de manière erronée comme il sera établi ultérieurement, la décision de réaliser une analyse de sang et de prendre une photographie des parties intimes de son enfant mineure contre les instructions expresses des deux parents, alors que ceux-ci étaient absents, constitue une ingérence dans le droit au respect de la vie privée de l'enfant et en particulier dans son droit à l'intégrité physique⁵⁹. Lorsqu'il s'agit d'un patient mineur, seule la personne investie de l'autorité parentale est habilitée à autoriser toute intervention médicale⁶⁰. Face au refus des parents d'autoriser un acte médical, seule l'urgence est de nature à justifier la décision de réaliser l'analyse de sang et de prendre les photographies⁶¹.

Droit d'accès et droit de copie. S'agissant de l'accès à des fichiers personnels détenus par des pouvoirs publics, en dehors du contexte des renseignements sensibles pour la sécurité nationale, les individus ont un intérêt primordial à obtenir les renseignements pour connaître et comprendre leur enfance et leurs années de formation ou pour retracer leur identité personnelle, s'agissant en particulier de leur filiation naturelle ou de renseignements sur les risques pour la santé auxquels ils ont été exposés. Dans ce contexte, les autorités doivent offrir aux intéressés une «procédure effective et accessible» qui leur permette d'avoir accès à «l'ensemble des informations pertinentes et appropriées». Le grand âge d'un individu accentue l'urgence à pouvoir retracer son parcours personnel⁶².

Dans le cadre d'une procédure d'attribution de la garde d'un enfant à la suite de la séparation de ses parents, le père souhaitait obtenir une copie d'un rapport établi par la Société pour la protection de l'enfance. Celle-ci a refusé de satisfaire à sa demande, le rapport étant confidentiel et destiné à la seule attention de la juridiction chargée de trancher le litige. Cette juridiction a rejeté sa demande d'accès excipant d'une absence d'intérêt légitime à prendre connaissance d'informations

⁵⁸ Cour eur. D.H., *Reklos et Davourlis c. Grèce*, 15 janvier 2009, req. n° 1234/05.

⁵⁹ Cour eur. D.H., *M.A.K. et R.K. c. Royaume-Uni*, 23 octobre 2010, req. n°s 45901/05 et 40146/06, § 75.

⁶⁰ Cour eur. D.H., *M.A.K. et R.K. c. Royaume-Uni*, 23 octobre 2010, req. n°s 45901/05 et 40146/06, § 77.

⁶¹ Cour eur. D.H., *M.A.K. et R.K. c. Royaume-Uni*, 23 octobre 2010, req. n°s 45901/05 et 40146/06, § 79.

⁶² Cour eur. D.H., *Haralambie c. Roumanie*, 27 octobre 2009, req. n° 21737/03, §§ 85-86, 93 et s.

concernant les données personnelles d'un mineur. La Cour a considéré que les informations contenues dans ce rapport étaient pertinentes pour le requérant et sa relation avec son fils, notant que si la juridiction avait estimé que l'intérêt de l'enfant imposait de ne pas l'éloigner de la mère, elle avait reconnu que le père faisait preuve d'une grande affection envers son fils, démontrée d'ailleurs par ses efforts persistants pour en obtenir la garde. La Cour a, dès lors, considéré que la communication du rapport lui aurait permis de prendre connaissance d'éventuels points négatifs contenus dans celui-ci et qui ont pu influencer la décision du tribunal et, le cas échéant, de les prendre en compte pour l'avenir afin d'améliorer sa relation avec son fils.

De plus, elle a noté que le requérant avait participé à l'élaboration du rapport et qu'il était donc légitime qu'il puisse connaître la manière dont les informations qu'il avait fournies avaient été analysées et prises en compte par la Société pour la protection de l'enfance. Par voie de conséquence, la Cour a jugé que le refus non motivé des autorités à consentir à la divulgation du rapport après la fin de la procédure s'analysait en une méconnaissance de l'obligation positive d'assurer le respect effectif du droit du requérant à sa vie privée et familiale, soulignant qu'il appartenait aux autorités nationales de démontrer l'existence de raisons impérieuses justifiant la non-divulgation au requérant d'un rapport contenant des informations personnelles le concernant directement⁶³.

Les informations personnelles relatives à un patient relèvent incontestablement de sa vie privée et la question de l'accès du patient à ces informations relève de l'article 8⁶⁴. La Cour a eu l'occasion de préciser que le droit d'un individu à accéder à des informations relatives à sa santé tombait dans la notion de vie privée⁶⁵. De même, l'exercice du droit à un accès effectif à l'information relative à la santé et à la possibilité de procréer est lié en tant que tel à la vie privée et familiale au sens de l'article 8⁶⁶. Pour rappel, l'accès des individus à des informations leur permettant d'évaluer les risques sanitaires auxquels ils ont été ou sont exposés entre dans le champ d'application de l'article 8.1⁶⁷.

Un détenu possède un intérêt à obtenir une copie du rapport établi après son examen médical à la clinique de la prison, ainsi que la page pertinente du registre relative à son admission dans cette clinique afin qu'il puisse être impliqué correctement dans le choix des soins de santé à lui prodiguer⁶⁸.

Lorsque des données à caractère personnel sont en cause, les obligations positives tirées de l'article 8 imposent, notamment, la mise à disposition de copies du dossier de données au profit de la personne concernée. Il peut revenir au déten-

⁶³ Cour eur. D.H., *Tsoulakis c. Grèce*, 15 octobre 2009, req. n° 50796/07, §§ 39-40 et 43-44.

⁶⁴ Cour eur. D.H., *Uslu c. Turquie (n° 2)*, 20 janvier 2009, req. n° 23815/04, § 22.

⁶⁵ Cour eur. D.H., *R.R. c. Pologne*, 26 mai 2011, req. n° 27.617/04, § 197.

⁶⁶ Cour eur. D.H., *K.H. et autres c. Slovaquie*, 28 avril 2009, req. n° 32881/04, § 44.

⁶⁷ Cour eur. D.H., *Dossi & autres c. Italie*, 12 octobre 2010, req. n° 26.053/07.

⁶⁸ Cour eur. D.H., *Uslu c. Turquie (n° 2)*, 20 janvier 2009, req. n° 23815/04, § 25.

teur du dossier de déterminer les modalités de reproduction du dossier et de dire que le coût doit en être supporté par la personne concernée. Toutefois, celle-ci ne devrait pas être obligée de justifier sa demande à obtenir une copie du dossier. C'est plutôt aux autorités de prouver qu'il existerait des raisons impérieuses de s'y opposer. À ce sujet, la Cour a indiqué qu'elle ne voyait pas comment la personne pourrait abuser des informations qui la concernent en faisant des photocopies des documents pertinents de son dossier médical, surtout lorsqu'elle avait déjà eu accès à la totalité de son contenu⁶⁹.

Le risque d'un abus par des tiers peut être évité autrement que par le refus de délivrer des copies du dossier médical à la personne concernée. Ainsi, la communication ou la divulgation de données à caractère personnel relatives à la santé incompatible avec les garanties de l'article 8 peut être évitée en incorporant dans le droit national des mesures appropriées visant à limiter strictement les circonstances dans lesquelles ces données peuvent être divulguées et les personnes susceptibles de pouvoir accéder aux dossiers⁷⁰.

Comme la condition et la santé d'un fœtus durant la grossesse sont des éléments de la santé de la femme enceinte, l'exercice effectif du droit d'accéder à des informations relatives à sa santé est souvent décisif pour l'exercice de l'autonomie personnelle (aussi couverte par l'article 8) en ce qu'il permet, sur la base de ces informations, de prendre des décisions à propos d'événements futurs relatifs à la qualité de vie de l'individu (comme par exemple refuser de consentir à un traitement médical ou demander de recevoir un traitement). L'importance d'accéder au moment adéquat à des informations relatives à la santé d'une personne est d'autant plus grande quand des évolutions rapides interviennent dans la condition de cette personne et que sa capacité à prendre des décisions pertinentes s'en trouve réduite. C'est encore plus vrai lorsque l'accès à des informations sur la santé de la mère et du fœtus est directement pertinent pour l'exercice de l'autonomie personnelle quand la législation autorise l'avortement dans certaines situations. Ainsi, lorsque la législation nationale autorise l'avortement en cas de malformation fœtale, il doit y avoir un cadre légal et procédural qui garantisse que des informations pertinentes, complètes et fiables sur la santé du fœtus soient disponibles à la femme enceinte⁷¹.

Collecte, conservation et utilisation de données. La mémorisation dans un registre secret et la communication de données relatives à la « vie privée » d'un individu entrent dans le champ d'application de l'article 8.1. De même, des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par

⁶⁹ Cour eur. D.H., *K.H. et autres c. Slovaquie*, 28 avril 2009, req. n° 32881/04, §§ 47-48 et 54.

⁷⁰ Cour eur. D.H., *K.H. et autres c. Slovaquie*, 28 avril 2009, req. n° 32881/04, § 56.

⁷¹ Cour eur. D.H., *R.R. c. Pologne*, 26 mai 2011, req. n° 27.617/04, §§ 197-200.

les pouvoirs publics⁷². Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne⁷³.

La collecte systématique et la conservation de données sur des individus par des services de sécurité constituent une ingérence dans leur vie privée, même lorsque ces données sont collectées dans un lieu public ou qu'elles concernent exclusivement les activités professionnelles ou publiques de ces personnes⁷⁴.

Mais, si la mémorisation, par une autorité publique, de données relatives à la vie privée d'un individu peut constituer une ingérence au sens de l'article 8, peu importe que les informations mémorisées soient ou non utilisées par la suite, la Cour tient compte, afin de déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée, 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 tirés⁷⁵.

Ainsi, dans l'affaire *Khelili c. Suisse*, la Cour a considéré que la mémorisation de données relatives à la vie privée de la requérante, dont faisait partie sa profession, ainsi que leur conservation, constituaient une ingérence au sens de l'article 8, car il s'agissait d'une donnée à caractère personnel se rapportant à un individu identifié ou identifiable. La Cour s'est alors référée aux principes dégagés dans l'affaire *S. et Marper c. Royaume-Uni* en matière de conservation d'informations à caractère personnel, ceux-ci reflétant les principes de base applicables aux traitements de données à caractère personnel (principe de finalité, de qualité et de durée de conservation des données, sans oublier leur sécurité). Dans ce cadre, la Cour a admis qu'il pouvait être conforme au principe de proportionnalité de conserver des données relatives à la vie privée d'une personne au motif que cette dernière pourrait récidiver. Toutefois, sans sous-estimer l'importance d'une prévention efficace de la criminalité, la Cour a considéré, eu égard, notamment, à l'importance primordiale de la présomption d'innocence dans une société démocratique, que le maintien de la mention «prostituée» comme profession de la requérante qui n'a jamais été condamnée pour exercice illicite de la prostitution ne répond pas à un «besoin social impérieux» au sens de l'article 8⁷⁶.

L'obligation faite à un individu d'indiquer sur sa carte d'imposition qu'il ne fait pas partie d'une église ou d'une société religieuse habilitées à prélever l'impôt culturel et se prévalant de ce droit, constitue une ingérence dans son droit au respect de sa vie privée⁷⁷.

⁷² Cour eur. D.H., *RAD c. Roumanie*, 9 juin 2009, req. n° 9742/04, § 34; Cour eur. D.H., *Wasmuth c. Allemagne*, 17 février 2011, req. n° 12884/03, § 74; 24 mai 2011, Cour eur. D.H., *Association «21 décembre 1989» et autres c. Roumanie*, 25 mai 2011, req. n°s 33.810/07 et 18.817/08, § 168.

⁷³ Cour eur. D.H., *RAD c. Roumanie*, 9 juin 2009, req. n° 9742/04, § 34.

⁷⁴ Cour eur. D.H., *Shimovolos c. Russie*, 11 juin 2011, req. n° 30.194/09, § 65.

⁷⁵ Cour eur. D.H., *Khelili c. Suisse*, 18 octobre 2011, req. n° 16.188/07, § 55.

⁷⁶ Cour eur. D.H., *Khelili c. Suisse*, 18 octobre 2011, req. n° 16.188/07, §§ 56, 61-62, 66 et 68.

⁷⁷ Cour eur. D.H., *Wasmuth c. Allemagne*, 17 février 2011, req. n° 12884/03, § 74.

Dans des circonstances normales, seule la destruction ou la rectification des informations personnelles conservées par des autorités représente une solution effective à une violation de l'article 8⁷⁸.

Intégrité personnelle, droit à la réputation et à l'honneur. L'intégrité personnelle ne se confond pas avec la réputation. La réputation est traditionnellement protégée par des lois sur la diffamation comme portant originellement sur des intérêts financiers ou le statut social. Par contre, les droits relatifs à l'intégrité personnelle qui relèvent de l'article 8 ne concernent pas l'évaluation externe des personnes alors que cette évaluation est décisive en matière de réputation. Il est possible de perdre l'estime de la société sans perdre l'intégrité qui est inaliénable⁷⁹.

La Cour a précisé que, dans sa jurisprudence, la réputation n'avait été reconnue que sporadiquement en tant que droit indépendant et que lorsque cela avait été le cas, c'était au motif que les allégations présentaient une nature sérieusement offensante dont la publication avait un effet direct inévitable sur la vie privée de l'individu concerné. Si ce dernier ne démontre pas qu'une publication constitue une ingérence sérieuse avec sa vie privée en manière telle qu'elle porte atteinte à son intégrité personnelle, il ne reste, dès lors, en jeu que sa seule réputation dans le cadre d'une publication qui doit être conforme à l'article 10 CEDH relatif à la liberté d'expression⁸⁰.

C'est dans cette mesure que l'article 8 englobe le droit à la protection de la réputation puisque la réputation d'une personne, même si celle-ci fait l'objet de critiques dans le contexte d'un débat public, fait partie de son identité personnelle et de son intégrité psychologique. La réputation relève, dès lors, également de sa vie privée, de la même façon que l'honneur⁸¹. Toutefois, pour que l'article 8 trouve à s'appliquer, l'attaque contre l'honneur personnel et la réputation doit atteindre un certain degré de gravité et, d'une certaine, manière causer un préjudice à la jouissance personnelle du droit au respect de la vie privée⁸². Pour le dire autrement, les allégations factuelles doivent être suffisamment graves et leur publication doit avoir des répercussions directes sur la vie privée de la personne concernée. Pour que l'article 8 entre en jeu, la publication pouvant ternir la réputation d'une personne doit constituer une atteinte à sa vie privée d'une gravité telle que son intégrité personnelle en soit compromise⁸³.

⁷⁸ Cour eur. D.H., *Kamburov c. Bulgarie*, 6 janvier 2011, req. n° 14.336/05, § 56. Ce ne sera donc pas toujours le cas, ce qui renvoie à la problématique des archives des anciens pays de l'Est comme la Bulgarie en l'espèce.

⁷⁹ Cour eur. D.H., *Karako c. Hongrie*, 28 avril 2009, req. n° 39311/05, §§ 22-23.

⁸⁰ Cour eur. D.H., *Karako c. Hongrie*, 28 avril 2009, req. n° 39311/05, § 23.

⁸¹ Cour eur. D.H., *A. c. Norvège*, 9 avril 2009, req. n° 28070/06, § 64; Cour eur. D.H., *Polanco Torres & Movilla Polanco c. Espagne*, 21 septembre 2010, req. n° 34147/06, § 40.

⁸² Cour eur. D.H., *A. c. Norvège*, 9 avril 2009, req. n° 28070/06, § 64.

⁸³ Cour eur. D.H., *Polanco Torres & Movilla Polanco c. Espagne*, 21 septembre 2010, req. n° 34147/06, § 40.

Les États ont l'obligation positive de protéger le droit à la réputation des individus, en ce qu'il s'agit d'un élément de leur vie privée au sens de l'article 8⁸⁴. Mais, l'article 8 ne permet pas de se plaindre d'une atteinte à la réputation qui est la conséquence prévisible de son comportement comme, par exemple, la commission d'un acte criminel⁸⁵.

Vie privée et liberté d'expression⁸⁶. Comme la notion de vie privée recouvre des éléments qui concernent l'identité d'une personne comme son nom ou son image⁸⁷, la publication de la photographie d'une personne relève de la vie privée⁸⁸, même lorsque celle-ci est une figure publique⁸⁹. La publication d'articles concernant une personne tombe aussi dans le champ de l'article 8⁹⁰.

La Cour distingue à cet égard entre les personnes « ordinaires » et les personnes « publiques » pour évaluer l'étendue du champ de la vie privée. Ainsi, s'agissant d'une personne « ordinaire », la zone d'interaction entre elle et des tiers qui, même dans un contexte public, peut relever de la vie privée, doit recevoir une interprétation élargie par rapport à celle qui serait reconnue à une personne « publique ». Le fait que la personne « ordinaire » soit poursuivie pénalement ne restreint pas le champ de cette protection offerte par l'article 8⁹¹.

L'ingérence dans le droit au respect de la vie privée liée à la publication d'une photographie doit s'apprécier en tenant compte de l'objet public ou privé de la question traitée, et de l'étendue de son usage⁹².

Ceci étant, l'article 8 peut contenir l'obligation positive de fournir une mesure de protection de la vie privée lors de l'exercice par des tiers de leur liberté d'expression. L'absence de recours lors de la publication d'informations relatives à des affaires privées peut constituer une violation du respect de la vie privée⁹³. Le cas échéant, la sévère limitation légale aux dommages et intérêts pour violation de la vie privée peut s'analyser en une violation de l'article 8⁹⁴.

⁸⁴ Pour un cas d'atteinte à la réputation par un rapport de police affirmant la culpabilité d'une personne en l'absence de poursuite pénale à son encontre, voy. : Cour eur. D.H., *Mikolajova c. Slovaquie*, 18 janvier 2011, req. n° 4479/03, § 53.

⁸⁵ Cour eur. D.H., *Mikolajova c. Slovaquie*, 18 janvier 2011, req. n° 4479/03, § 57.

⁸⁶ Voy. également *supra*, « Notion de vie privée ».

⁸⁷ Cour eur. D.H., *Wolfgang Schüssel c. Autriche*, 21 février 2002, req. n° 42409/98 (la Cour était saisie du recours introduit par l'ancien premier ministre autrichien qui se plaignait d'une affiche électorale reprenant son visage sur la moitié duquel était surimposé celui de Jorg Haider).

⁸⁸ Cour eur. D.H., *Khuzin et autres c. Russie*, 23 octobre 2008, req. n° 13470/02; Cour eur. D.H., *Pfeifer c. Autriche*, 15 novembre 2007, req. n° 12556/03; Cour eur. D.H., *Gourguenidze c. Géorgie*, 17 octobre 2006, req. n° 71678/01; Cour eur. D.H., *White c. Suède*, 19 septembre 2006, req. n° 42435/02; Cour eur. D.H., *Sciacca c. Italie*, 11 janvier 2005, req. n° 50774/99 (la requérante se plaignait de la diffusion de sa photographie à l'occasion d'une conférence de presse organisée par le parquet italien et la garde des finances).

⁸⁹ Cour eur. D.H., *Pfeifer c. Autriche*, 15 novembre 2007, req. n° 12556/03.

⁹⁰ Cour eur. D.H., *White c. Suède*, 19 septembre 2006, req. n° 42435/02.

⁹¹ Cour eur. D.H., *Sciacca c. Italie*, 11 janvier 2005, req. n° 50774/99.

⁹² Cour eur. D.H., *Gourguenidze c. Géorgie*, 17 octobre 2006, req. n° 71678/01.

⁹³ Cour eur. D.H., *Wolfgang Schüssel c. Autriche*, 21 février 2002, req. n° 42409/98.

⁹⁴ Cour eur. D.H., 25 novembre 2008, *Biriuk c. Lituanie*, req. n° 23373/03; Cour eur. D.H., *Armonas c. Lituanie*, 25 novembre 2008, req. n° 36919/02.

Par ailleurs, la liberté d'expression englobe (aussi) la publication de photographies⁹⁵. Reprenant la distinction entre les personnes « ordinaires » et les personnes « publiques », la Cour a précisé que la liberté d'expression n'appelait pas d'interprétation élargie lorsque la personne concernée était inconnue du public. Elle a ajouté que les limites de la critique admissible à son égard ne pouvaient pas être aussi larges que lorsqu'il s'agissait d'une personnalité publique qui s'expose inévitablement et consciemment à un contrôle attentif de ses faits et gestes et qui devait dès lors montrer une plus grande tolérance par rapport à cette critique⁹⁶.

Lorsque la publication d'articles et de photographies tombe dans le champ de la vie privée, il faut mettre en balance sa protection et la liberté d'expression⁹⁷, tout en distinguant les personnes « ordinaires » des personnes « publiques ». La Cour a cependant tempéré l'impact de cette distinction en affirmant que toute personne, même connue du grand public, devait pouvoir bénéficier d'une « espérance légitime » de protection et de respect de la vie privée⁹⁸. Elle a noté de plus qu'une vigilance accrue quant à la protection de la vie privée s'imposait face aux progrès techniques d'enregistrement et de reproduction de données personnelles d'un individu⁹⁹.

Dans la mise en balance du droit au respect de la vie privée et de la liberté d'expression, la Cour a rappelé qu'elle avait toujours mis l'accent sur la contribution que la parution de photos ou d'articles dans la presse apportait au débat d'intérêt général dans son appréciation de la balance¹⁰⁰.

S'agissant de l'affaire *Caroline de Monaco*, la Cour a estimé que la publication des photographies et articles ayant eu pour seul objet de satisfaire la curiosité d'un certain public sur les détails de sa vie privée, ne saurait passer pour contribuer à un quelconque débat d'intérêt général pour la société, malgré sa notoriété et que, dès lors, la liberté d'expression appelait une interprétation moins large. Elle a repris ce critère d'utilité pour le débat d'intérêt général pour la société dans l'affaire *Biriuk* relative à la publication d'un article sur l'état de santé de la requérante qui contenait également des références sur sa vie sexuelle¹⁰¹. En l'espèce, elle a souligné le fait que la publication visant à satisfaire la curiosité lubrique d'un certain lectorat et les intérêts commerciaux du journal, n'y contribuait en rien. La Cour a également appliqué ce critère dans l'affaire *Khuzin*¹⁰² où la police russe avait communiqué à un journaliste la photographie du passeport du requérant sans son accord, qui l'a utilisée dans une émission télévisée sur les procédures

⁹⁵ Cour eur. D.H., *Gourguenidze c. Géorgie*, 17 octobre 2006, req. n° 71678/01.

⁹⁶ Cour eur. D.H., *Gourguenidze c. Géorgie*, 17 octobre 2006, req. n° 71678/01. Dans le même sens, Cour eur. D.H., *Petrina c. Roumanie*, 14 octobre 2008, req. n° 78060/01.

⁹⁷ Cour eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, req. n° 59320/00; Cour eur. D.H., *White c. Suède*, 19 septembre 2006, req. n° 42435/02.

⁹⁸ Cour eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, req. n° 59320/00.

⁹⁹ Cour eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, req. n° 59320/00.

¹⁰⁰ Cour eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, req. n° 59320/00; en ce sens également : Cour eur. D.H., *Gourguenidze c. Géorgie*, 17 octobre 2006, req. n° 71678/01.

¹⁰¹ Cour eur. D.H., *Biriuk c. Lituanie*, 25 novembre 2008, req. n° 23373/03.

¹⁰² Cour eur. D.H., *Khuzin et autres c. Russie*, 23 octobre 2008, req. n° 13470/02.

criminelles en cours. La Cour a considéré que, comme cela n'apportait aucune plus-value informationnelle, il devait y avoir une raison impérieuse pour justifier l'ingérence dans la vie privée du requérant. En l'espèce, elle a jugé qu'il n'y avait aucune raison légitime en ce sens d'autant que le requérant n'était pas un fugitif recherché puisqu'il était en prison, et que, son procès n'ayant pas encore débuté, cela ne pouvait pas renforcer la publicité de la procédure judiciaire.

Notons que la Cour considère et a répété à maintes reprises que les journalistes ont un rôle clé en qualité de « chien de garde ». Ce faisant, la Cour souligne qu'il n'existe pas de hiérarchie entre les droits garantis par ces articles 8 et 10 de la Convention¹⁰³.

La Cour insiste, par ailleurs, sur le rôle prééminent de la presse dans l'information du public et dans la diffusion d'informations et d'idées dans des matières d'intérêt public, dans un État de droit. Non seulement la presse a la tâche de diffuser ces informations et idées mais le public a aussi le droit de les recevoir. Autrement, la presse ne serait pas en mesure de jouer son rôle vital de « chien de garde »¹⁰⁴.

Ainsi, pour savoir si un État a atteint un juste équilibre entre le droit au respect de la vie privée d'un individu et la liberté d'expression du journal, la Cour prend en compte l'obligation positive de l'État tirée de l'article 8 de protéger la vie privée d'individus visés dans des procédures pénales en cours, ainsi que la liberté de la presse de communiquer des informations sur un sujet d'intérêt public en ce compris les procédures pénales en cours, et le droit du public de recevoir cette information¹⁰⁵.

Dans l'affaire *A. c. Norvège*, la Cour a jugé que l'État devait se voir reconnaître une large marge d'appréciation dans l'évaluation du besoin de protéger la vie privée du requérant par rapport à la sauvegarde de la liberté d'expression du journal¹⁰⁶.

C'est dans le cas de débats ou de questions d'intérêt public général que l'étendue de la critique acceptable est plus grande envers des politiciens ou toutes autres figures publiques que pour des particuliers, dès lors que les premiers, au contraire des seconds, se sont exposés volontairement à un contrôle plus attentif de leurs faits et gestes tant par les journalistes que par le public en général et qu'ils doivent, dès lors, montrer une plus grande tolérance¹⁰⁷.

La Cour a également rappelé la distinction entre la constatation de faits et les jugements de valeurs, soulignant que si l'existence de faits pouvait être démon-

¹⁰³ Cour eur. D.H., *Timciuc c. Roumanie*, 12 octobre 2010, req. n° 28.999/03, § 144.

¹⁰⁴ Cour eur. D.H., *Mosley c. Royaume-Uni*, 10 mai 2011, req. n° 48009/08, § 112.

¹⁰⁵ Cour eur. D.H., *A. c. Norvège*, 9 avril 2009, req. n° 28070/06, § 65. Voy. aussi: Cour eur. D.H., *Polanco Torres & Movilla Polanco c. Espagne*, 21 septembre 2010, req. n° 34147/06, § 41.

¹⁰⁶ Cour eur. D.H., *A. c. Norvège*, 9 avril 2009, req. n° 28070/06, § 66.

¹⁰⁷ Cour eur. D.H., *Petrenco c. Moldavie*, 30 mars 2010, req. n° 20928/05, § 55. Voy. aussi: Cour eur. D.H., *Timciuc c. Roumanie*, 12 octobre 2010, req. n° 28.999/03, § 150.

trée, les jugements de valeur n'étaient pas susceptibles de preuve. Dès lors, l'exigence de prouver la véracité d'un jugement de valeur était impossible à rencontrer et violait la liberté d'expression. La Cour a précisé que la distinction entre la constatation d'un fait et le jugement de valeur relevait de la marge d'appréciation des autorités nationales et, en particulier, des juridictions nationales. Cependant, même en présence d'un jugement de valeur, il doit exister une base factuelle suffisante pour le fonder, sinon il serait excessif¹⁰⁸.

La Cour a aussi distingué la constatation de faits, même controversés, susceptibles de contribuer à un débat d'intérêt public général dans une société démocratique, par rapport à des allégations sordides sur la vie privée d'un individu. En ce qui concerne les premiers, le rôle prééminent de la presse dans une démocratie et sa tâche d'agir en tant que « chien de garde » sont des considérations importantes en faveur d'une conception restrictive à toute limite à la liberté d'expression. Par contre, la presse à sensation qui vise à satisfaire la curiosité d'un certain lectorat sur les aspects de la vie privée de certaines personnes ne mérite pas la même protection que celle conférée par l'article 10 à la presse. En conséquence, dans ce type d'affaires, la liberté d'expression appelle une interprétation plus étroite¹⁰⁹.

Ceci étant, la liberté journalistique comprend aussi la possibilité de recourir à un certain degré d'exagération voire de provocation¹¹⁰.

Dans l'affaire *Palade c. Roumanie*, le requérant se plaignait d'avoir été surnommé « Gogu le Boucher » après avoir tué plusieurs personnes, les avoir découpées en morceaux et éparpillé ces derniers dans des poubelles de la ville. La Cour a rappelé que le droit au respect de la vie privée du requérant devait être mis en balance avec l'intérêt public de la liberté d'expression, intérêt dans lequel les journalistes ont un rôle clé en qualité de « chien de garde »¹¹¹.

Elle a aussi indiqué que si les juridictions judiciaires étaient bien les lieux de détermination de la culpabilité ou de l'innocence d'un individu poursuivi pénalement, cela ne signifiait pas qu'il ne pouvait pas y avoir de débat préalable ou contemporain à ce sujet dans d'autres lieux, que ce soit dans des journaux spécialisés, dans la presse en général ou dans le public. Toutefois, les commentaires admissibles sur des procédures pénales en cours ne peuvent pas s'étendre à ceux qui sont susceptibles de porter préjudice, que ce soit intentionnellement ou non, aux chances d'un individu à un procès équitable, ou qui sont de nature à porter atteinte à la confiance du public dans le rôle des juridictions judiciaires dans l'administration de la justice¹¹².

¹⁰⁸ Cour eur. D.H., *Petresco c. Moldavie*, 30 mars 2010, req. n° 20928/05, § 56.

¹⁰⁹ Cour eur. D.H., *Mosley c. Royaume-Uni*, 10 mai 2011, req. n° 48009/08, § 114.

¹¹⁰ Cour eur. D.H., *Palade c. Roumanie*, 31 août 2010, req. n° 37441/05, § 28.

¹¹¹ Cour eur. D.H., *Palade c. Roumanie*, 31 août 2010, req. n° 37441/05, § 27.

¹¹² Cour eur. D.H., *Palade c. Roumanie*, 31 décembre 2010, req. n° 37441/05, § 27. Voy. aussi: Cour eur. D.H., *Timciuc c. Roumanie*, 12 octobre 2010, req. n° 28.999/03, § 146.

La diffusion d'images des ébats sexuels du président de la fédération internationale de l'automobile a donné l'occasion à la Cour de rappeler que la publication d'articles, de photographies et d'images vidéo d'un individu participant à des actes sexuels avait un impact significatif sur son droit au respect de la vie privée¹¹³.

Comme les médias audiovisuels ont un effet plus immédiat et plus puissant que les médias imprimés et bien que la liberté d'expression comprenne aussi la publication de photographies, la Cour a rappelé que, dans ce cas, la protection des droits d'autrui revêt une importance particulière, notamment quand les images contiennent des informations très personnelles et très intimes d'un individu ou quand elles ont été prises dans un lieu privé et clandestinement en recourant à des équipements d'enregistrement secrets. Les éléments pertinents à prendre en compte pour apprécier l'équilibre entre les intérêts concurrents résident dans la contribution complémentaire que pourrait apporter la publication de ces photographies à un débat d'intérêt général, ainsi que le contenu de ces photographies¹¹⁴.

B. COUR DE JUSTICE DE L'UNION EUROPÉENNE

L'application du droit fondamental à la protection de la vie privée et des données à caractère personnel. Les juridictions européennes montrent des approches différentes lorsqu'il s'agit d'évaluer des ingérences dans le droit à la protection des données et/ou de la vie privée.

Dans son arrêt *Volker und Markus Schecke & Eifert*¹¹⁵, la Cour cherche à appliquer conjointement les articles 7 et 8 de la Charte, en référence à la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8. Elle affirme alors, en se fondant sur les arrêts *Amann*¹¹⁶ et *Rotaru*¹¹⁷, que la protection offerte par la Charte dans ses articles 7 et 8, s'applique à toute information concernant une personne physique identifiée ou identifiable¹¹⁸ et que dès lors, les personnes morales ne peuvent se prévaloir de cette protection sauf dans la mesure où le nom légal de la personne morale identifie une ou plusieurs personnes physiques¹¹⁹. Ce qui l'amène à considérer que la publication sur Internet de données nominatives concernant les personnes physiques bénéficiaires d'aides agricoles constitue une ingérence dans leur droit au respect de la vie privée reconnu à l'article 7, et

¹¹³ Cour eur. D.H., *Mosley c. Royaume-Uni*, 10 mai 2011, req. n° 48009/08, § 71.

¹¹⁴ Cour eur. D.H., *Mosley c. Royaume-Uni*, 10 mai 2011, req. n° 48009/08, § 115.

¹¹⁵ C.J.U.E. (GC), 9 novembre 2011, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, C-92/09 et C-93/09. Voy. E. DEGRAVE, « Arrêt "Volker und Markus Schecke et Eifert" : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.*, 2011, pp. 97-99 et I. ANDOULSI, « L'arrêt de la Cour du 9 novembre 2012 dans les affaires jointes *Volker und Markus Schecke GbR et Hartmut Eifert c. Land d'Hessen* : une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles ? », *C.D.E.*, vol. 47, n° 2, 2011, pp. 471-522.

¹¹⁶ Cour eur. D.H., *Amann c. Suisse*, 16 février 2000, req. n° 27798/95.

¹¹⁷ Cour eur. D.H., *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95.

¹¹⁸ C.J.E.U. (GC), 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, point 52.

¹¹⁹ *Ibid.*, point 53.

un traitement de données relevant de la protection garantie par l'article 8 de la Charte¹²⁰. Si cette ingérence peut être considérée comme poursuivant un but légitime, à savoir l'accroissement de la transparence de l'utilisation des fonds communautaires de la PAC¹²¹, elle sera finalement jugée disproportionnée par la Cour¹²².

Le Tribunal de la fonction publique, dans son arrêt *V c. Parlement*, a opté pour une application de l'article 8 CEDH (en sus d'une interprétation des dispositions pertinentes du règlement 45/2001). Le litige soulevait la question de la légalité du transfert de la Commission au Parlement d'un dossier médical archivé concernant une candidate à un poste d'agent contractuel au sein de la seconde institution, et écartée du recrutement sur le fondement de ce dossier médical pour raisons d'inaptitude sans que de nouveaux examens médicaux n'aient été accomplis¹²³. Le Tribunal y rappelle la jurisprudence de la Cour eur. D.H. selon laquelle la vie privée comporte le droit de tenir son état de santé secret¹²⁴. Il considère que le transfert entre institutions de données relatives à la santé d'une personne constitue une ingérence dans sa vie privée, et ce quelle que soit l'utilisation ultérieure des données communiquées¹²⁵. Si le Tribunal semble exprimer des doutes sur le fait qu'une telle ingérence soit valablement « prévue par la loi » compte tenu des termes très généraux en lesquels sont prévus les transferts entre institutions¹²⁶, il poursuivra son raisonnement en affirmant que la réalisation d'un examen d'embauche sert bien un intérêt légitime des institutions de l'Union susceptible de justifier une telle ingérence¹²⁷. En revanche, compte tenu du caractère extrêmement intime et sensible des données à caractère médical¹²⁸, il juge en l'espèce que « cet intérêt ne justifie pas que l'on procède à un transfert de données médicales d'une institution à une autre sans le consentement de l'intéressé »¹²⁹, car le Parlement aurait pu satisfaire sa mission dans des conditions moins attentatoires.

Enfin, dans l'affaire *Scarlet*, la Cour ne fera pas application du droit à la protection des données de la Charte, se contentant d'affirmer qu'un système de filtrage des communications électroniques aux fins d'empêcher l'échange de fichiers portant

¹²⁰ *Ibid.*, points 58 et 60.

¹²¹ *Ibid.*, point 71.

¹²² *Ibid.*, point 86.

¹²³ T.F.P., 5 juillet 2011, *V c. Parlement*, aff. F-46/09; voy. également F. OMRANI et J.-M. VAN GYSEGHEM, « Quand le transfert des données "santé" est illégal », note sous T.F.P. (1^{re} ch.), 7 juillet 2011, *R.D.T.I.*, 2011, pp. 121-149.

¹²⁴ T.F.P., 5 juillet 2011, *V c. Parlement*, aff. F-46/09, point 111.

¹²⁵ *Ibid.*, point 112.

¹²⁶ En effet, tandis que la condition de légalité du transfert est supposée reposer sur l'article 7 du règlement 45/2001, le Tribunal soutient au point 117 que « l'article 7 du règlement n° 45/2001 prévoit dans des termes très généraux que les transferts de données entre institutions ne sont possibles que si les données communiquées "sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire", et que "la question se pose de savoir si cet article est libellé avec suffisamment de précision pour permettre aux destinataires de la loi de régler leur conduite et répond à l'exigence de prévisibilité dégagée par la jurisprudence de la Cour européenne des droits de l'homme" ».

¹²⁷ T.F.P., 5 juillet 2011, *V c. Parlement*, aff. F-46/09, point 120.

¹²⁸ *Ibid.*, point 123.

¹²⁹ *Ibid.*, point 125.

atteinte aux droits d'auteurs *est susceptible de porter atteinte* à ce droit fondamental protégé en son article 8¹³⁰.

Il convient également de relever l'arrêt du 20 mai 2003 dans lequel la Cour opère une analyse du lien entre la directive 95/46 et l'article 8 de la Convention européenne des droits de l'homme en ces termes :

« 70. La directive 95/46 elle-même, tout en ayant pour objectif principal de garantir la libre circulation des données à caractère personnel, prévoit, à son article 1^{er}, paragraphe 1, que "les États membres assurent [...] la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel". Plusieurs considérants de ladite directive, notamment les dixième et onzième, expriment également cette même exigence.

71. À cet égard, il y a lieu de relever que l'article 8 de la CEDH, tout en énonçant, à son paragraphe 1, le principe de non-ingérence des autorités publiques dans l'exercice du droit à la vie privée, admet, à son paragraphe 2, qu'une telle ingérence est possible pour autant qu'elle soit "prévues 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".

72. Aussi, pour les besoins de l'application de la directive 95/46, et, en particulier, de ses articles 6, paragraphe 1, sous c), 7, sous c) et e), et 13, importe-t-il de vérifier, en premier lieu, si une réglementation telle que celle en cause dans les affaires au principal prévoit une ingérence dans la vie privée et, le cas échéant, si cette ingérence est justifiée au regard de l'article 8 de la CEDH »¹³¹. ■

Les paragraphes qui suivent portent plus spécifiquement sur la jurisprudence relative à la protection des données à caractère personnel, principalement en lien avec la directive 95/46 du Parlement européen 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 évoquée dans la première partie de la présente contribution.

Données à caractère personnel. Conduites à interpréter des dispositions de la directive 95/46 ou du règlement 45/2001, les juridictions de l'Union ont eu à vérifier au préalable, de manière plus ou moins évidente, si elles se trouvaient effectivement en présence d'un traitement de données à caractère personnel soumis auxdites réglementations.

¹³⁰ C.J.U.E., 24 novembre 2011, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, point 50. Voy. D. GOBERT et J. JOURET, « L'arrêt *Scarlet contre Sabam* : la consécration d'un juste équilibre du rôle respectif de chaque acteur dans la lutte contre les échanges illicites d'œuvres protégées sur Internet », *R.D.T.I.*, 2012, pp. 33 et s.

¹³¹ C.J.U.E., 20 mai 2003, *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01, points 70 et s.

C'est ainsi qu'elles ont eu l'occasion de confirmer que les noms et prénoms¹³² peuvent être considérés comme des données à caractère personnel, mais aussi l'adresse¹³³, et que la communication de telles données constitue un traitement¹³⁴. Le Tribunal de première instance a lui aussi établi, au soutien de la Commission européenne, que les noms et prénoms des fonctionnaires européens ou des personnes figurant sur les listes de réserve des concours généraux européens constituaient des données à caractère personnel¹³⁵, au détriment de la position du requérant qui soutenait que l'information selon laquelle une personne est fonctionnaire ne peut pas être considérée comme relevant de sa vie privée¹³⁶. La Cour a établi que la publication de données à caractère personnel sur Internet, en l'espèce les noms des bénéficiaires d'aides agricoles au titre de la PAC, constituait bien un traitement de données¹³⁷, mais aussi la transmission par un exploitant de réseau de télécommunications attribuant des numéros de téléphone de données à caractère personnel concernant ses abonnés à une entreprise tierce fournisseur de services de renseignements téléphoniques accessibles au public¹³⁸. Conduite à interpréter l'étendue du droit d'accès des individus aux informations concernant les destinataires de données à caractère personnel en cas de communication (voy. *infra*), la Cour a explicité que l'information sur les destinataires ou les catégories de destinataires auxquels des données à caractère personnel sont communiquées ainsi que le contenu de ces dernières sont à distinguer des données à caractère personnel de base traitées, et constituent des informations relatives au traitement¹³⁹. Enfin, il faut souligner que bien que la Cour n'ait pas procédé à l'application des articles 7 et 8 de la Charte dans l'affaire *Scarlet* (voy. *supra*), elle a néanmoins procédé à la reconnaissance des adresses IP des utilisateurs à l'origine de l'envoi de contenus illicites sur le réseau, comme données à caractère personnel relatives à ces utilisateurs, dans la mesure où leur collecte et traitement visent à les identifier précisément¹⁴⁰.

La Cour a également considéré que les données « qui concernent tant les revenus alloués par certaines entités que les bénéficiaires de ceux-ci, constituent des données à caractère personnel au sens de l'article 2, sous a), de la directive 95/46, puisqu'il s'agit d'« informations concernant une personne physique identifiée ou identifiable » »¹⁴¹.

Données sensibles. La Cour a considéré, au sujet de données à caractère personnel relatives à la santé, qu'« il convient de donner à l'expression “données

¹³² C.J.U.E., 29 juin 2010, *Bavarian Lager c. Commission*, C-28/08 P, point 86.

¹³³ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 42.

¹³⁴ C.J.U.E., 29 juin 2010, *Bavarian Lager c. Commission*, C-28/08 P, point 86.

¹³⁵ T.P.I., 7 juillet 2011, *Jordana c. Commission*, T-161/04, point 91.

¹³⁶ T.P.I., 7 juillet 2011, *Jordana c. Commission*, T-161/04, point 60.

¹³⁷ C.J.U.E. (GC), 9 novembre 2011, *Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen*, C-92/09 et C-93/09, point 60.

¹³⁸ C.J.U.E., 5 mai 2011, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, C-543/09, point 53.

¹³⁹ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 43.

¹⁴⁰ C.J.U.E., 24 novembre 2011, *Scarlet c. SABAM*, C-70/10, point 51.

¹⁴¹ C.J.U.E., 20 mai 2003, *Rechnungshof et autres c. Österreichischer Rundfunk et autres*, C-465/00, C-138/01 et C-139/01, point 64.

relatives à la santé” employée à son article 8, paragraphe 1, une interprétation large de sorte qu’elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d’une personne» et que «l’indication du fait qu’une personne s’est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l’article 8, paragraphe 1, de la directive 95/46»¹⁴².

L’article 8, paragraphe 1, de la directive 95/46 est donc applicable dès l’instant où un traitement porte sur les données relatives à la santé même si ce traitement ne vise pas les données à caractère personnel pour ce qu’elles sont.

Par exemple, le site Internet d’une société comprend un annuaire des personnes travaillant en son sein ; annuaire accompagné de leurs photos. Si un des employés apparaît sur la photo en portant des lunettes correctrices, le traitement de cette photo, étant une donnée à caractère personnel, devrait tomber dans le champ d’application de l’article 8, paragraphe 1 – impliquant des conditions de traitement plus strictes – dès lors que la donnée est relative à la santé alors même qu’il importe peu au responsable de traitement que cette personne soit myope ou pas.

Il eût été plus opportun de ne viser le contenu des données à caractère personnel relatives à la santé que si elles sont traitées *pour ce qu’elles révèlent ou contiennent*.

Traitement. Les juridictions européennes ont eu l’occasion de se prononcer sur la notion de traitement. Ainsi, La Cour a considéré que «le transfert des données PNR au CBP constitue un traitement ayant pour objet la sécurité publique et les activités de l’État relatives à des domaines du droit pénal»¹⁴³.

Dans l’arrêt *Lindqvist*, la Cour a rappelé que «la notion de “traitement” de [données à caractère personnel] employée à l’article 3, paragraphe 1, de la directive 95/46, elle comprend, conformément à la définition figurant à l’article 2, sous b), de celle-ci, “toute opération ou ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données à caractère personnel”» et que «l’opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d’autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un “traitement de données à caractère personnel, automatisé en tout ou en partie,” au sens de l’article 3, paragraphe 1, de la directive 95/46»¹⁴⁴.

¹⁴² C.J.U.E., 6 novembre 2003, *Lindqvist*, C-101/01, points 50 et s.

¹⁴³ C.J.U.E., 30 mai 2006, *Parlement européen c. Contrôleur européen de la protection des données (CEPD)*, C-317/04 et C-318/04, point 56. Par la suite, la Cour a considéré qu’un tel traitement était hors du champ d’application de la directive 95/46 dès lors qu’il s’agissait de sécurité publique et d’activités de l’État relatives à des matières de droit pénal.

¹⁴⁴ C.J.U.E., 6 novembre 2003, *Lindqvist*, C-101/01, point 25.

Dans un autre arrêt, la Cour a précisé sa pensée en considérant que l'enregistrement et l'utilisation des données à caractère personnel par un responsable de traitement « ainsi que leur transmission au Rechnungshof et leur insertion par ce dernier dans un rapport destiné à être communiqué à diverses instances politiques et largement diffusé, présentent le caractère d'un traitement de données à caractère personnel au sens de l'article 2, sous b), de [la directive 95/46] »¹⁴⁵.

Sur question préjudicielle posée par la Cour administrative suprême de Finlande, la Cour a considéré que :

- « (...) l'article 3, paragraphe 1, de la directive doit être interprété en ce sens qu'une activité qui consiste à :
- collecter dans les documents publics de l'administration fiscale des données relatives aux revenus du travail et du capital ainsi qu'au patrimoine de personnes physiques et à les traiter en vue de leur publication,
 - les publier dans l'ordre alphabétique et par classe de revenus, sous la forme de listes détaillées établies commune par commune,
 - les céder sous la forme de disques CD-ROM, pour qu'elles soient utilisées à des fins commerciales,
 - les traiter dans un service de SMS qui permet aux utilisateurs de téléphones mobiles, en envoyant le nom et la commune de résidence d'une personne, de recevoir des informations concernant les revenus du travail et du capital ainsi que le patrimoine de cette personne,
 - doit être considérée comme un "traitement de données à caractère personnel" au sens de cette disposition »¹⁴⁶. ■

La notion de traitement doit donc être analysée de façon très large et recouvre un large faisceau d'opérations effectuées sur les données à caractère personnel allant de la collecte initiale à la destruction en passant par le classement. À noter que le fait d'anonymiser une donnée, la faisant ainsi sortir du champ d'application de la directive 95/46, constitue également un traitement au sens de l'article 3, paragraphe 1 de la directive.

L'exercice d'activités exclusivement personnelles ou domestiques. Dans l'arrêt *Lindqvist*, la Cour a précisé que « des activités bénévoles ou religieuses, ne sont pas assimilables [la notion d'activités exclusivement personnelles ou domes-

¹⁴⁵ C.J.U.E., 20 mai 2003, *Rechnungshof et autres c. Österreichischer Rundfunk et autres*, C-465/00, C-138/01 et C-139/01, point 64.

¹⁴⁶ C.J.U.E., 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, C-73/07, point 37. Sur cet arrêt, voy. C. DE TERWANGNE, « Les dérogations à la protection des données en faveur de journalisme enfin élucidées », note sous C.J.C.E. (GC), 16 décembre 2008, *Satakunnan Markkinapörssi Oy et Satamedia Oy*, aff. C-73/07, R.D.T.I., 2010, n° 38, pp. 132-146 ; E. CRUYSMANS, « Le traitement de données à caractère personnel effectué à des fins de journalisme : la consécration de la liberté d'expression », *A&M*, 2013, pp. 270 et s.

tiques] et ne sont donc pas couvertes par cette exception»¹⁴⁷. Elle a poursuivi en considérant que «Cette exception doit donc être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes»¹⁴⁸.

Exceptions à des fins de journalisme. La Cour a eu l'occasion de se prononcer sur la question de l'exception liée aux activités de journalisme dans un arrêt du 16 décembre 2008 en considérant que «les dérogations prévues à l'article 9 de la directive s'appliquent non seulement aux entreprises de média, mais également à toute personne exerçant une activité de journalisme»¹⁴⁹ et que «le fait qu'une publication de données à caractère public soit liée à une fin lucrative n'exclut *a priori* pas qu'elle puisse être considérée comme une activité "aux seules fins de journalisme". En effet, ainsi que le relèvent Markkinapörssi et Satamedia dans leurs observations et M^{me} l'avocat général au point 82 de ses conclusions, toute entreprise cherche un profit par son activité. Un certain succès commercial peut même constituer la condition *sine qua non* de la subsistance d'un journalisme professionnel»¹⁵⁰.

À l'occasion de cet arrêt, la Cour a également eu l'occasion de se prononcer sur le moyen de diffusion de l'information en considérant qu'il «n'est pas déterminant pour apprécier s'il s'agit d'une activité "aux seules fins de journalisme"»¹⁵¹.

Elle a donc conclu que des activités «concernant des données provenant de documents publics selon la législation nationale, peuvent être qualifiées d'"activités de journalisme", si elles ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit. Elles ne sont pas réservées aux entreprises de média et peuvent être liées à un but lucratif»¹⁵².

La notion de finalités journalistiques doit donc être vue de manière large et susceptible d'englober de nombreux acteurs répondant à la condition de finalité fixée par la Cour.

Intérêt légitime du responsable de traitement. Dans l'affaire *ASNEF*, il s'agissait pour la Cour de déterminer si l'article 7, sous f) de la directive relatif à la nécessité d'un traitement sur le fondement de l'intérêt légitime du responsable du

¹⁴⁷ C.J.U.E., 6 novembre 2003, *Lindqvist*, C-101/01, points 45 et s.

¹⁴⁸ C.J.U.E., 6 novembre 2003, *Lindqvist*, C-101/01, points 45 et s.

¹⁴⁹ C.J.U.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*, C-73/07, point 58.

¹⁵⁰ *Ibid.*, point 59.

¹⁵¹ *Ibid.*, point 60.

¹⁵² C.J.U.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*, C-73/07, point 61.

traitement¹⁵³ s'opposait à l'exigence de la réglementation espagnole selon laquelle une telle base de légitimité ne puisse jouer que pour des données figurant dans des sources accessibles au public, telles que définies dans le droit national.

La Cour a tout d'abord considéré que l'article 7 de la directive 95/46 prévoyait « une liste exhaustive et limitative des cas dans lesquels un traitement de données peut être considéré comme licite »¹⁵⁴, excluant dès lors la possibilité pour les États membres de prévoir en dehors des cas énumérés, de nouvelles bases de légitimité, ou bien d'en modifier la portée en prévoyant des exigences supplémentaires¹⁵⁵. Elle reconnaît néanmoins que l'article 7, sous f) de la directive qui prévoit deux conditions cumulatives à la nécessité du traitement, à savoir la réalisation d'un intérêt légitime du responsable de traitement et le respect des droits et libertés fondamentaux de la personne concernée, appelle à une pondération des droits et intérêts en cause¹⁵⁶. Si la Cour admet que les États membres disposent d'une marge d'appréciation pour l'établissement de principes directeurs utiles à ladite pondération¹⁵⁷, et que « la gravité de l'atteinte aux droits fondamentaux de la personne concernée par ledit traitement peut varier en fonction du fait de savoir si les données en cause figurent déjà, ou non, dans des sources accessibles au public »¹⁵⁸, l'article 7, sous f) « s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées »¹⁵⁹, en l'espèce des données qui ne figureraient pas dans des sources accessibles au public. Enfin, la Cour considère que l'article 7, sous f) est une disposition qui remplit les conditions de précision pour lui reconnaître un effet direct¹⁶⁰.

Droit d'accès des individus dans le temps. Dans l'affaire *Rijkeboer*, la Cour a eu l'occasion d'apporter une interprétation tout à fait éclairante de la portée dans le temps du droit d'accès consacré à l'article 12, sous a) de la directive, et plus particulièrement du droit d'accès aux informations portant sur *les destinataires ou les catégories de destinataires* auxquels les données à caractère personnel de l'individu ont été communiquées, appelés en langage informatique *log files*. La Cour a affirmé que le droit au respect de la vie privée « implique que la personne concernée puisse s'assurer que [...] les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés »¹⁶¹. Contre les avis exprimés par le requérant au principal devant le Conseil d'État des Pays-Bas et de plusieurs États membres, la Cour a considéré que pour assurer l'effet utile des autres droits

¹⁵³ Cet article dispose que le traitement de données à caractère personnel est licite s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée [...].

¹⁵⁴ C.J.U.E., 24 novembre 2011, *ASNEF – FECEMD c. Administración del Estado*, C-468/10 et C-469/10, point 30.

¹⁵⁵ C.J.U.E., 24 novembre 2011, *ASNEF – FECEMD c. Administración del Estado*, C-468/10 et C-469/10, point 32.

¹⁵⁶ *Ibid.*, point 40.

¹⁵⁷ *Ibid.*, point 46.

¹⁵⁸ *Ibid.*, point 44.

¹⁵⁹ C.J.U.E., 24 novembre 2011, *ASNEF – FECEMD c. Administración del Estado*, C-468/10 et C-469/10, points 48-49.

¹⁶⁰ C.J.U.E., 24 novembre 2011, *ASNEF – FECEMD c. Administración del Estado*, C-468/10 et C-469/10, point 55.

¹⁶¹ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 49.

octroyés par la directive aux individus, à savoir ses droits de rectification, d'opposition et de recours en cas de dommage¹⁶², le droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi que sur le contenu des données communiquées « doit nécessairement concerner le passé »¹⁶³. Aux fins de déterminer l'étendue de ce droit d'accès dans le passé, et dès lors de fixer la durée de conservation des informations portant sur les destinataires, les États membres sont tenus de prendre en considération plusieurs paramètres : la durée de conservation des données de base¹⁶⁴ ; les dispositions de droit national relatives aux délais de recours ; la nature plus ou moins sensible des données ; le nombre et la fréquence des communications à des destinataires¹⁶⁵ ; et plus généralement le caractère proportionné de la charge de l'obligation de conservation pour les responsable de traitement¹⁶⁶. En l'espèce, la Cour a jugé qu'« [u]ne réglementation nationale limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement »¹⁶⁷.

Obligations administratives du responsable de traitement. La Cour a jugé que l'article 18, § 2 de la directive 95/46, qui prévoit la possibilité pour le responsable du traitement de voir ses obligations administratives de notification simplifiées lorsqu'il nomme un détaché à la protection des données, n'impose aucune obligation à ce dernier de tenir un registre contenant les informations relatives au traitement préalablement à la mise en œuvre dudit traitement¹⁶⁸. Elle a en outre précisé que « la directive 95/46 ne soumet pas les traitements de données à caractère personnel à un contrôle préalable généralisé »¹⁶⁹, ne prévoyant la possibilité pour les États membres de procéder à des examens avant leur mise en œuvre que des *traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées* en application de l'article 20, § 1^{er}.

Indépendance des autorités de contrôle. Réunie en grande chambre, la Cour était saisie d'une requête de la Commission européenne contre l'Allemagne visant à établir le manquement de cet État à son obligation au titre de l'article 28 de la directive 95/46 relatif à l'indépendance des autorités de contrôle¹⁷⁰. Il s'agis-

¹⁶² Ces droits sont consacrés aux articles 12, sous b) et c), 14, 22 et 23.

¹⁶³ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 54 ; Voy. aussi C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E. (3^e ch.), 7 mai 2009, *R.D.T.I.*, n° 43/2011, pp. 65-81.

¹⁶⁴ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 58.

¹⁶⁵ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 63.

¹⁶⁶ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, points 62-63.

¹⁶⁷ C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, point 66.

¹⁶⁸ C.J.U.E. (GC), 9 novembre 2011, *Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen*, C-92/09 et C-93/09, point 101.

¹⁶⁹ C.J.U.E. (GC), 9 novembre 2011, *Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen*, C-92/09 et C-93/09, point 104.

¹⁷⁰ C.J.U.E. (GC), 9 mars 2010, *Commission c. République fédérale d'Allemagne*, C-518/07.

sait de déterminer si les autorités de contrôle du secteur non public instituées au niveau des Länders et soumises à une tutelle exercée par l'État étaient compatibles avec la directive 95/46 qui prévoit que les autorités de contrôle (sans distinction du secteur public ou non public), « exercent en toute indépendance les missions dont elles sont investies ». La Cour étend la question de l'indépendance des autorités de contrôle de la directive 95/46 au règlement 45/2001, établissant que : « [l']article 44 du règlement 45/2001 et l'article 28 de la directive 95/46 sont fondés sur le même concept général, il convient d'interpréter ces deux dispositions de manière homogène, de sorte que non seulement l'indépendance du CEPD¹⁷¹, mais aussi celle des autorités nationales, impliquent l'absence de toute instruction relative à l'exercice de leurs missions »¹⁷². Elle considère, contre la position soutenue par l'Allemagne, que « rien n'indique que l'exigence d'indépendance concerne exclusivement la relation entre les autorités de contrôle et les organismes soumis à leur contrôle »¹⁷³, jugeant alors que « 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 [...] »¹⁷⁴. Ce qui lui permet de conclure que l'Allemagne a manqué à son obligation en vertu de l'article 29 de la directive 95/46 en soumettant les autorités de contrôle du secteur non public à la tutelle de l'État¹⁷⁵.

Jean-Marc Van Gyseghem

Directeur de l'Unité de recherche « Libertés et société de l'information »
du Centre de Recherches Information, Droit et Société (www.crids.eu)
et avocat Barreau de Bruxelles (www.rawlingsgiles.be)

Cécile de Terwangne

Professeur à la Faculté de Droit de l'Université de Namur
et Directrice du master complémentaire D.T.I.C. (www.crids.eu)
et de la Chaire E-Gouvernement de l'Université de Namur

Jean Herveg

Chargé d'enseignement à l'Université de Namur, Directeur de Recherche
au Centre de Recherches Information, Droit et Société (www.crids.eu),
avocat au barreau de Bruxelles (www.rawlingsgiles.be)

Claire Gayrel

Chercheuse senior au Centre de Recherches Information,
Droit et Société (www.crids.eu)

¹⁷¹ Contrôleur européen de protection des données.

¹⁷² C.J.U.E. (GC), 9 mars 2010, *Commission c. République fédérale d'Allemagne*, C-518/07, point 28.

¹⁷³ C.J.U.E. (GC), 9 mars 2010, *Commission c. République fédérale d'Allemagne*, C-518/07, point 19.

¹⁷⁴ C.J.U.E. (GC), 9 mars 2010, *Commission c. République fédérale d'Allemagne*, C-518/07, point 30.

¹⁷⁵ C.J.U.E. (GC), 9 mars 2010, *Commission c. République fédérale d'Allemagne*, C-518/07, point 56.