La protection des données à caractère personnel en droit européen

Personal data protection in European law

Claire Gayrel, Jean Herveg et Jean-Marc Van Gyseghem[1]

Résumé

La présente chronique dédiée à la protection de la vie privée et des données à caractère personnel au niveau des Cours de justice européennes et de la Cour européenne des droits de l'homme couvre les années 2012 et 2013.

Cependant et compte tenu de l'actualité jurisprudentielle des juridictions de l'Union européenne, la partie de la chronique qui lui est consacrée couvre également les six premiers mois de l'année 2014. En effet, cette période est marquée par deux arrêts fondamentaux, et très remarqués, rendus par la Cour de justice, qui outre leur intérêt dans le domaine de la protection des données, marquent également l'évolution de la Cour de Luxembourg dans sa fonction de juge des droits fondamentaux. Il s'agit de la décision Digital Rights Ireland *portant annulation de la directive 2006/24 relative à la conservation des données de trafic et de la décision* Google Spain *consacrant, dans certaines limites, un droit à l'oubli numérique.*

La chronique révèle un travail jurisprudentiel important en matière de protection des données à caractère personnel en Europe, ce qui démontre une préoccupation de plus en plus grande en cette matière. Certaines décisions ont délimité de manière intéressante et motivée les atteintes à la liberté fondamentale qu'est le droit à la vie privée. L'on doit certainement s'en réjouir.

Abstract

This Column presents the evolutions that have marked the years 2012 and 2013 in the field of private life and personal data before the European Court of Justice and the European Court of Human Rights.

However, given the importance of the case law of EU jurisdictions this column also covers the first six months of 2014. Two ECJ cases have been particularly important. Beyond their interest for the subject of data protection, the two cases mark the evolution of the ECJ's role in adjudicating fundamental rights disputes. The first is Digital Rights Ireland, *regarding the annulment of the data retention Directive 2006/24, and* Google Spain *recognizing, within certain limits, a right to be forgotten.*

The Column reveals the many questions raised in the field of personal data protection in Europe. Some decisions have interestingly delimited the notion of breaches in the fundamental right to privacy. These evolutions must be welcomed.

[1] La présente contribution ne reflète que les opinions personnelles des auteurs qui remercient cependant les chercheurs du Crids pour les discussions fructueuses en matière de protection des données à caractère personnel.

Claire Gayrel, Jean Herveg et Jean-Marc Van Gyseghem

I. La Cour européenne des droits de l'homme

1. La protection des droits et libertés et l'exécution des obligations internationales des États

Les États demeurent responsables au regard de la Convention même lorsqu'ils se conforment à leurs obligations juridiques internationales et que ces dernières trouvent leur origine dans leur appartenance à une organisation internationale à laquelle ils ont transféré une partie de leur souveraineté[2]. La justification des mesures prises en conformité avec ces obligations internationales est présumée lorsque l'organisation internationale protège les droits fondamentaux de manière comparable à celle offerte par la Convention, tant au niveau des garanties matérielles que des mécanismes de contrôle de leur respect. Dans la mesure où cette protection équivalente est considérée comme étant offerte par l'organisation internationale, il est présumé que l'État n'a pas manqué à ses obligations au regard de la Convention quand il ne fait qu'implémenter les obligations juridiques qui dérivent de son appartenance à cette organisation[3]. Néanmoins, l'État reste totalement responsable au regard de la Convention pour tous les actes pris en dehors de ses obligations juridiques internationales notamment quand il exerce un pouvoir d'appréciation dans leur mise en œuvre. De plus, la présomption de conformité peut être renversée lorsque, eu égard aux circonstances particulières d'un cas d'espèce, il est considéré que la protection des droits est insuffisante. Dans de telles hypothèses, le rôle de la Convention d'instrument constitutionnel d'ordre public européen prime sur l'intérêt de la coopération internationale[4]. La Cour a déjà considéré que l'Union européenne offrait, en principe, une protection des droits fondamentaux équivalente à celle de la Convention[5].

2. Le droit de pouvoir établir les détails de son identité personnelle

Le respect de la vie privée exige que chacun puisse établir les détails de son identité d'être humain et le droit d'un individu à de telles informations est essentiel du fait de leurs incidences sur la formation de la personnalité[6].

Le droit de connaître son ascendance entre dans le champ de la vie privée qui englobe des aspects importants de l'identité personnelle dont l'identité des géniteurs fait partie[7]. Les individus ont un droit à l'identité et à l'épanouissement personnel, ainsi que celui de nouer et de développer des relations avec ses semblables et le monde extérieur. Deux éléments participent notamment à l'épanouissement

[2] Cour eur. D.H., arrêt *Michaud c. France*, 6 décembre 2012, req. n° 12323/11, § 102.
[3] *Idem*, § 103.
[4] *Idem*, § 103.
[5] *Idem*, § 105.
[6] Cour eur. D.H., arrêt *A.M.M. c. Roumanie*, 14 février 2012, req. n° 2151/10, § 51.
[7] Cour eur. D.H., arrêt *Godelli c. Italie*, 25 septembre 2012, req. n° 33783/09, § 45. Voy. aussi l'arrêt *Röman c. Finlande*, 29 janvier 2013, req. n° 13072/05, § 43 (cette affaire concerne des délais de forclusion pour agir en recherche de paternité), et l'arrêt *Laakso c. Finlande*, 15 janvier 2013, req. n° 7361/05, § 38.

personnel des individus. D'abord, l'établissement des détails de son identité d'être humain et l'intérêt vital à obtenir des informations nécessaires à la découverte de la vérité concernant un aspect important de son identité personnelle, comme l'identité de ses géniteurs. À cet égard, la naissance, et singulièrement les circonstances de celle-ci, relève de la vie privée de l'enfant, puis de l'adulte[8].

Mais, la question de l'accès à ses origines et de la connaissance de l'identité de ses parents biologiques n'est pas de même nature que celle de l'accès au dossier personnel établi sur un enfant pris en charge ou de la recherche des preuves d'une paternité alléguée[9]. D'un côté, il y a le droit de l'enfant à la connaissance de ses origines. De l'autre, il y a l'intérêt de la mère à conserver l'anonymat pour sauvegarder sa santé en accouchant dans des conditions médicales appropriées, sans oublier la question de l'intérêt général dans le souci de protéger la santé de la mère et de l'enfant lors de la grossesse et de l'accouchement et d'éviter des avortements clandestins ou des abandons sauvages[10]. À cet égard, la Cour a rappelé que les États devaient pouvoir choisir les moyens qu'ils estiment les plus adaptés pour assurer équitablement la conciliation entre la protection de la mère et la demande légitime de l'intéressée à avoir accès à ses origines dans le respect de l'intérêt général[11].

Dans l'affaire *Godelli c. Italie*, la Cour a noté que la requérante n'avait eu accès à aucune information sur sa mère et sa famille biologique lui permettant d'établir quelques racines que ce soit de son histoire dans le respect de la préservation des intérêts des tiers. Sans une pesée des droits et des intérêts en présence et sans aucune possibilité de recours, la requérante s'est vue opposer un refus absolu et définitif d'accéder à ses origines personnelles[12]. De plus, l'intérêt que peut avoir une personne à connaître son ascendance ne cesse nullement avec l'âge, bien au contraire[13]. En l'absence de toute possibilité reconnue à l'enfant adopté dont la mère biologique a décidé de garder l'anonymat et non reconnu à la naissance, de demander soit l'accès à des informations non identifiantes sur ses origines, soit la réversibilité du secret, la Cour a jugé qu'il n'y avait pas d'équilibre et de proportionnalité entre les intérêts des parties concernées[14].

Les procédures en matière de paternité tombent dans le champ de l'article 8[15]. En matière de recherche de paternité, il faut un juste équilibre entre le droit du requérant (mineur) de voir ses intérêts protégés dans la procédure afin de dissiper son incertitude quant à son identité personnelle et le droit de son père présumé de ne pas participer à la procédure, ni de subir des tests de paternité[16].

---

[8] Cour eur. D.H., arrêt *Godelli c. Italie*, 25 septembre 2012, req. n° 33783/09, § 46.
[9] *Idem*, § 62.
[10] *Idem*, §§ 63-64.
[11] *Idem*, § 67.
[12] *Idem*, § 68.
[13] *Idem*, § 69.
[14] *Idem*, § 71.
[15] Cour eur. D.H., *Röman c. Finlande*, 29 janvier 2013, req. n° 13072/05, § 43. Cette affaire concerne des délais de forclusion pour agir en recherche de paternité. Voy. aussi l'arrêt *Laakso c. Finlande*, 15 janvier 2013, req. n° 7361/05, § 38.
[16] Cour eur. D.H., arrêt *A.M.M. c. Roumanie*, 14 février 2012, req. n° 2151/10, § 64. Voy. aussi en matière d'établissement et de contestation de paternité : Cour eur. D.H., arrêt *Ahrens c. Allemagne*, 22 mars 2012, req. n° 45071/09 ; arrêt *Kautzor c. Allemagne*, 22 mars 2012, req. n° 23338/09 ; arrêt *K.A.B. c. Espagne*, 10 avril 2012, req. n° 59819/08.

3. Le droit à un nom patronymique unique

La Cour a rappelé que le nom, en tant qu'élément d'individualisation principal d'une personne au sein de la société, appartient au noyau dur des considérations relatives au droit au respect de la vie privée et familiale[17]. La personne a un intérêt primordial à avoir un nom unique[18].

4. Le changement de nom patronymique

Le choix ou le changement de prénom ou de nom tombe dans le champ de l'article 8[19]. Des restrictions à ce sujet peuvent être justifiées dans l'intérêt public comme pour assurer l'exactitude d'un registre de la population, protéger les moyens d'identification personnelle ou relier à une famille les porteurs d'un nom donné[20]. La Cour admet qu'il est de l'intérêt public de garantir la stabilité du nom de famille, en vue de la sécurité juridique des rapports sociaux. Elle a rappelé à cet égard que le nom conserve un rôle déterminant pour l'identification des personnes[21]. Il incombe aux autorités nationales de fournir les raisons pertinentes et suffisantes qui justifieraient le refus d'autoriser le changement de nom par un individu[22].

5. Le droit de conserver son nom de jeune fille

Le refus des autorités d'autoriser une épouse de porter uniquement son nom de jeune fille alors que l'époux est autorisé à conserver son propre nom, est une discrimination basée sur le sexe[23].

6. La protection contre la divulgation d'informations personnelles

La notion de vie privée est un concept large qui n'est pas susceptible de définition exhaustive et qui recouvre, entre autres choses, les informations relatives à l'identité personnelle comme le nom de la personne, sa photographie ou son intégrité physique et morale. Cette notion s'étend de manière générale aux informations personnelles dont les individus sont légitimement en droit de s'attendre à ce qu'elles ne soient pas publiées sans leur consentement[24]. À cet égard, lorsque des valeurs fondamentales et des aspects essentiels de la vie privée sont en jeu et

[17] Cour eur. D.H., arrêt *Henry Kismoun c. France*, 5 décembre 2013, req. nº 32265/10, § 36.
[18] Voy. à ce sujet : Cour eur. D.H., arrêt *Henry Kismoun c. France*, 5 décembre 2013, req. nº 32265/10, § 36.
[19] Cour eur. D.H., arrêt *Garnaga c. Ukraine*, 16 mai 2013, req. nº 20390/07, § 29. Voy. aussi la décision *De Ram c. France,* 27 août 2013, req. nº 38275/10, § 19.
[20] Cour eur. D.H., arrêt *Garnaga c. Ukraine*, 16 mai 2013, req. nº 20390/07, § 38 ; arrêt *Henry Kismoun c. France*, 5 décembre 2013, req. nº 32265/10, § 31.
[21] Cour eur. D.H., arrêt *Henry Kismoun c. France*, 5 décembre 2013, req. nº 32265/10, § 32.
[22] Cour eur. D.H., arrêt *Garnaga c. Ukraine*, 16 mai 2013, req. nº 20390/07, § 39.
[23] Cour eur. D.H., arrêt *Leventoglu Abdulkadiroglu c. Turquie*, 28 mai 2013, req. nº 7971/07 ; arrêt *Tuncer Günes c. Turquie*, 3 septembre 2013, req. nº 26268/08 ; arrêt *Tanbay Tüten c. Turquie*, 10 décembre 2013, req. nº 38249/09.
[24] Cour eur. D.H., arrêt *Axel Springer c. Allemagne*, 7 février 2012, req. nº 39954/08, § 83 ; arrêt *Ageyevyv c. Russie*, 18 avril 2013, req. nº 7075/10, § 193 ; arrêt *Von Hannover c. Allemagne (n° 3)*, 19 septembre 2013, req. nº 8772/10, § 41.

qu'une dissuasion effective est nécessaire, celle-ci peut être atteinte en premier par des incriminations pénales et leur mise en œuvre effective par le biais d'investigations et de poursuites pénales[25].

7. La divulgation d'informations relatives à la santé

Les informations personnelles relatives à un patient appartiennent à sa vie privée[26]. La Cour considère qu'il est primordial d'avoir des règles claires et détaillées en matière de divulgation d'informations médicales confidentielles et qui offrent des garanties suffisantes contre le risque d'abus et d'arbitraire[27]. La Cour répète à cet égard que la protection des données à caractère personnel, en ce compris les informations médicales, est d'une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale[28].

8. Le droit d'accès

Une requérante se plaignait de ne pas avoir eu accès aux données collectées à son sujet par les services secrets polonais durant l'ère communiste. La Cour a rappelé que conformément à sa jurisprudence constante, l'enregistrement de données relatives à la vie privée d'un individu dans un registre secret et sa divulgation tombaient dans le champ de l'article 8, § 1er[29].

L'État doit offrir une procédure effective et accessible permettant à une personne d'obtenir un accès complet au fichier créé par les services secrets communistes à son sujet afin de pouvoir contester les allégations relatives à sa collaboration avec ces services. La procédure doit permettre à la personne d'avoir accès à toutes les informations pertinentes et appropriées qui lui permettraient de contester effectivement toute allégation de collaboration avec les services secrets. De même, cette procédure doit lui offrir la possibilité de corriger toutes les entrées erronées dans les fichiers pertinents[30] et notamment de pouvoir contester sa classification par les services de sécurité comme étant leur informateur secret[31].

De même, l'État a une obligation positive d'offrir une procédure effective et accessible permettant à une personne d'avoir accès dans un délai raisonnable à l'ensemble des informations recueillies à propos de son père décédé par les anciens services de sécurité communistes et qui se trouvaient encore en possession des autorités publiques[32].

---

[25] Cour eur. D.H., arrêt *Ageyevyy c. Russie*, 18 avril 2013, req. n° 7075/10, § 196 (dans le cas d'espèce, la Cour a jugé que l'État avait manqué à son obligation d'investiguer et de poursuivre les divulgations non autorisées d'informations confidentielles relatives au statut d'une personne adoptée).
[26] *Idem*, § 30.
[27] *Idem*, § 37.
[28] *Idem*, § 45.
[29] Cour eur. D.H., arrêt *Joanna Szulc c. Pologne*, 13 novembre 2012, req. n° 43932/08, § 85.
[30] *Idem*, § 87.
[31] *Idem*, § 94.
[32] Cour eur. D.H., arrêt *Antoneta Tudor c. Roumanie*, 24 septembre 2013, req. n° 23445/04, § 39.

9. L'accès à des informations permettant d'évaluer les risques pour la santé

Les États ont l'obligation de fournir un accès aux informations essentielles permettant aux individus d'évaluer les risques pour leur santé et pour leur vie[33]. Cette obligation peut aussi comprendre l'obligation de fournir ces informations[34].

Ainsi, l'État doit veiller à ce que les personnes qui pratiquent la plongée sous-marine reçoivent les informations essentielles à propos des tables de décompression afin qu'elles puissent évaluer les risques pour leur santé et leur sécurité[35]. De même, l'État doit prendre les mesures législatives nécessaires afin de garantir que les médecins prennent en considération les conséquences prévisibles d'une intervention médicale programmée sur l'intégrité physique de leurs patients et de les en informer au préalable de manière à ce que ces derniers soient mis en mesure de donner un consentement éclairé. En particulier, il s'ensuit que si un risque prévisible de cette nature se réalise sans que le patient n'en ait été dûment informé par les médecins, l'État concerné pourra être tenu directement responsable pour ce manque d'information[36].

10. La protection des communications

Le droit au respect de la vie privée protège la confidentialité des communications privées, peu importe leur contenu ou leur forme. Ceci signifie que l'article 8 protège la confidentialité de tous les échanges qui peuvent intervenir entre des individus à des fins de communication[37].

11. La surveillance secrète des individus

La simple existence d'une législation autorisant les surveillances secrètes constitue une ingérence dans le droit au respect de la vie privée[38]. Ce type de législation doit offrir une protection suffisante contre l'arbitraire et la surveillance indiscriminée[39], ce qui n'est pas le cas :

– en l'absence d'un organe indépendant qui contrôle la mise en œuvre des mesures de surveillance ainsi que la destruction des informations collectées dans le délai imparti lorsque la surveillance s'est avérée infructueuse ;

[33] Cour eur. D.H., arrêt *Vilnes et autres c. Norvège*, 5 décembre 2013, req. nos 52806/09 et 22703/10, § 235. Voy. aussi l'arrêt *Csoma c. Roumanie*, 15 janvier 2013, req. no 8759/05, § 42.
[34] Cour eur. D.H., arrêt *Vilnes et autres c. Norvège*, 5 décembre 2013, req. nos 52806/09 et 22703/10, § 235.
[35] *Idem*, § 245.
[36] Cour eur. D.H., arrêt *Csoma c. Roumanie*, 15 janvier 2013, req. no 8759/05, § 42.
[37] Cour eur. D.H., arrêt *Michaud c. France*, 6 décembre 2012, req. no 12323/11, § 90.
[38] Cour eur. D.H., arrêt *Hadzhiev c. Bulgarie*, 23 octobre 2012, req. no 22373/04, § 44 (voy. aussi l'arrêt *Natzev c. Bulgarie*, 16 octobre 2012, req. no 27079/04 et l'arrêt *Lenev c. Bulgarie*, 4 décembre 2012, req. no 41452/07, § 144).
[39] Cour eur. D.H., arrêt *Hadzhiev c. Bulgarie*, 23 octobre 2012, req. no 22373/04, § 45. Voy. aussi l'arrêt *Lenev c. Bulgarie,* 4 décembre 2012, req. no 41452/07, § 146 ; l'arrêt *Acatrinei c. Roumanie*, 25 juin 2013, req. no 18540/04, § 58 et l'arrêt *Niculescu c. Roumanie*, 25 juin 2013, req. no 25333/03, § 99.

– en l'absence de mesures de sécurité suffisantes en matière de surveillance réalisée pour des motifs de sécurité nationale et non pas dans le contexte de procédures pénales ;
– en l'absence de dispositions suffisamment précises indiquant la procédure à suivre pour l'examen et la conservation des informations collectées ainsi que pour leur destruction ;
– en l'absence d'un organe indépendant supervisant et rapportant le fonctionnement du système de surveillance secrète ;
– en l'absence d'un contrôle indépendant sur l'usage des informations collectées en dehors du champ initial des mesures de surveillance ;
– en l'absence d'information des personnes concernées alors que celle-ci peut être faite sans mettre en péril l'objectif de la surveillance.

12. Les écoutes téléphoniques

Les communications téléphoniques sont comprises dans les notions de « vie privée » et de « correspondance » au sens de l'article 8[40]. Leur interception, leur mémorisation dans un registre secret et la communication de données relatives à la vie privée d'un individu sont des ingérences d'une autorité publique dans l'exercice du droit au respect de la vie privée[41], ainsi que leur utilisation éventuelle dans le cadre de poursuites pénales[42]. Il importe peu que ce soit au domicile de l'individu ou à son bureau[43].

Les écoutes téléphoniques et autres équivalents constituent des ingérences graves dans la vie privée et la correspondance. En conséquence, la base légale doit être particulièrement précise. Il est essentiel d'avoir des règles claires et détaillées en la matière d'autant que la technologie est continuellement de plus en plus sophistiquée[44]. Selon la jurisprudence constante de la Cour, la législation nationale doit fixer[45] :

– les catégories d'infractions pouvant justifier la mesure de surveillance ;
– les catégories de personnes susceptibles d'avoir leurs téléphones mis sous surveillance ;
– la durée maximale des écoutes téléphoniques ;
– la procédure à suivre pour l'examen, l'utilisation et la conservation des informations collectées ;

[40] Cour eur. D.H., arrêt *Alony Kate c. Espagne*, 17 janvier 2012, req. n° 5612/08, § 73 (voy. aussi l'arrêt *Draksas c. Lituanie*, 31 juillet 2012, req. n° 36662/04, § 52 ; l'arrêt *Acatrinei c. Roumanie*, 25 juin 2013, req. n° 18540/04, § 57 ; l'arrêt *Niculescu c. Roumanie*, 25 juin 2013, req. n° 25333/03, § 98 ; l'arrêt *Balteanu c. Roumanie*, 16 juillet 2013, req. n° 142/04, § 41, et l'arrêt *Ulariu c. Roumanie*, 19 novembre 2013, req. n° 19267/05, § 46).
[41] Cour eur. D.H., arrêt *Alony Kate c. Espagne*, 17 janvier 2012, req. n° 5612/08, § 73 ; arrêt *Bucur et Toma c. Roumanie*, 8 janvier 2013, req. n° 40238/02, § 162 ; arrêt *Ulariu c. Roumanie*, 19 novembre 2013, req. n° 19267/05, § 46.
[42] Cour eur. D.H., décision *Cariello c. Italie*, 30 avril 2013, req. n° 14064/07, § 49 ; décision *D'Auria et Balsamo*, 11 juin 2013, req. n° 11625/07, § 27 ; arrêt *Ulariu c. Roumanie*, 19 novembre 2013, req. n° 19267/05, § 46.
[43] Cour eur. D.H., arrêt *Savovi c. Bulgarie*, 27 novembre 2012, req. n° 7222/05, § 52.
[44] Cour eur. D.H., arrêt *Sefilyan c. Arménie*, 2 octobre 2012, req. n° 22491/08, § 124. Voy. aussi l'arrêt *Alony Kate c. Espagne*, 17 janvier 2012, req. n° 5612/08, § 76.
[45] Cour eur. D.H., arrêt *Sefilyan c. Arménie,* 2 octobre 2012, req. n° 22491/08, § 125.

– les précautions à prendre pour communiquer ces informations à d'autres personnes ;
– les circonstances dans lesquelles les enregistrements pouvaient ou devaient être effacés ou détruits.

Il faut, de plus, une mesure de protection légale contre l'ingérence arbitraire des autorités publiques dans les droits garantis par l'article 8. À cet effet, la loi doit indiquer l'étendue des pouvoirs conférés aux autorités compétentes et la manière de les exercer, avec suffisamment de clarté, en tenant compte de l'objectif légitime de la mesure, et ce afin de donner aux individus une protection adéquate contre les ingérences arbitraires[46].

L'exigence de prévisibilité de l'interception des communications pour des raisons d'investigations policières ne signifie pas que l'individu doive savoir quand les autorités vont effectivement intercepter ses communications afin qu'il puisse adapter son comportement en conséquence. Toutefois, la loi doit être rédigée en des termes suffisamment clairs pour donner aux citoyens des indications appropriées sur les circonstances et les conditions dans lesquelles les autorités publiques sont autorisées à recourir à cette ingérence secrète et potentiellement dangereuse dans le droit au respect de la vie privée et de la correspondance[47].

On ne doit pas restreindre la possibilité de mettre sous écoute téléphonique un suspect au seul motif que les lignes téléphoniques dont il est titulaire sont également utilisées par d'autres personnes[48]. Lorsque des contacts ont lieu entre un suspect et des tiers, il est loisible aux autorités de mettre sous écoute aussi les lignes téléphoniques appartenant aux tiers concernés, à condition que cette ingérence soit justifiée par un besoin impérieux[49].

Les droits tirés de l'article 8 par une personne ne sont pas concrètement affectés lorsqu'il s'agit de l'enregistrement des conversations téléphoniques entre des parties tierces auxquelles cette personne n'était pas partie même si ces conversations téléphoniques mentionnent son implication dans des activités criminelles[50].

13. La publication dans la presse du contenu d'écoutes téléphoniques

La publication dans la presse d'extraits de conversations de nature strictement privée et n'ayant que très peu de rapports avec les accusations portées contre le

[46] *Idem*, § 126. Voy. aussi : Cour eur. D.H., arrêt *Savovi c. Bulgarie*, 27 novembre 2012, req. n° 7222/05, § 55 ; l'arrêt *Balteanu c. Roumanie*, 16 juillet 2013, req. n° 142/04, § 42 et l'arrêt *Ulariu c. Roumanie*, 19 novembre 2013, req. n° 19267/05, § 49.
[47] Cour eur. D.H., arrêt *Sefilyan c. Arménie*, 2 octobre 2012, req. n° 22491/08, § 123.
[48] Cour eur. D.H., décision *Cariello c. Italie*, 30 avril 2013, req. n° 14064/07, § 63 ; décision *D'Auria et Balsamo*, 11 juin 2013, req. n° 11625/07, § 41.
[49] Cour eur. D.H., décision *Cariello c. Italie*, 30 avril 2013, req. n° 14064/07, § 63.
[50] Cour eur. D.H., décision *Fesiuc c. Roumanie*, 4 juin 2013, req. n° 25497/04, §§ 71 et s. Ceci n'empêche pas que la question soit traitée sous l'angle de l'article 6.

requérant, voire aucun, ne correspond à aucun besoin social impérieux[51]. Il appartient aux États d'organiser leurs services et de former leur personnel de manière à garantir qu'aucune information confidentielle ou secrète ne soit divulguée[52]. La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel qui ne serait pas conforme aux garanties prévues à l'article 8. En cas de défaillance de la protection des renseignements confidentiels ou secrets, les autorités doivent ouvrir une enquête effective afin de remédier, dans la mesure du possible, à la situation, notamment en poursuivant les éventuels responsables de l'indiscrétion commise[53]. Le devoir de mener une enquête effective ne saurait être compris comme une obligation de résultat[54].

Comme la procédure à suivre pour les écoutes téléphoniques est sujette à un contrôle judiciaire rigoureux, il est logique que les résultats de celles-ci ne soient pas rendus publics sans un contrôle judiciaire tout aussi strict[55].

14. Les perquisitions et saisies de données informatiques

La notion de domicile couvre les locaux résidentiels et peut être étendue à des locaux professionnels ou commerciaux. Cela ne concerne pas que les bureaux d'un particulier mais également ceux d'une personne morale en ce compris ses succursales et autres locaux commerciaux. Les ingérences dans des activités ou des locaux professionnels ou commerciaux peuvent être plus étendues que dans les autres hypothèses[56].

La perquisition et la saisie des fichiers informatiques d'un bureau d'avocats constituent une ingérence dans le droit au respect de la correspondance[57]. Le droit interne et la pratique doivent fournir des protections adéquates et effectives contre les abus et l'arbitraire. En particulier, il faut vérifier si la perquisition a été autorisée par un juge et qu'elle est justifiée par des motifs raisonnables.

L'objet de la perquisition doit être raisonnablement délimité. Lorsqu'il s'agit de perquisitionner un bureau d'avocats, la perquisition doit être réalisée en présence d'un observateur indépendant afin que les éléments protégés par le secret professionnel ne soient pas emportés[58]. Concrètement, la police ne devrait pouvoir consulter et saisir que les fichiers informatiques en relation avec les raisons pour

[51] Cour eur. D.H., arrêt *Casuneanu c. Roumanie*, 16 avril 2013, req. nº 22018/10, § 79.
[52] *Idem*, § 81.
[53] *Idem*, § 84.
[54] *Idem*, § 86.
[55] *Idem*, § 92.
[56] Cour eur. D.H., arrêt *Bernh Larsen Holding AS et autres c. Norvège*, 14 mars 2013, req. nº 24117/08, § 104.
[57] Cour eur. D.H., arrêt *Robathin c. Autriche*, 3 juillet 2012, req. nº 30457/06, § 39.
[58] Cour eur. D.H., arrêt *Robathin c. Autriche*, 3 juillet 2012, req. nº 30457/06, § 44.

lesquelles la perquisition a été autorisée et non pas tous les fichiers informatiques sans distinction aucune.

En matière de contrôle fiscal, lorsque plusieurs entreprises partagent un même serveur sans que leurs archives ne soient clairement séparées, il est raisonnable de considérer que les autorités fiscales n'ont pas à s'en remettre aux indications des personnes contrôlées pour trouver les informations sur un serveur mais qu'elles doivent pouvoir avoir accès à toutes les données reprises sur le serveur afin de procéder elles-mêmes au tri des données[59].

15. La prise et la conservation de matériel cellulaire ainsi que la réalisation et la conservation de profils ADN

La prise et la conservation de matériel cellulaire ainsi que la réalisation et la conservation de profils ADN, constituent des ingérences dans le droit au respect de la vie privée[60]. La loi interne doit offrir des protections appropriées pour prévenir tout usage des données à caractère personnel qui ne serait pas conforme avec les garanties de l'article 8. Le besoin de ces protections est d'autant plus grand lorsqu'il s'agit de la protection de données à caractère personnel sujettes à des traitements automatisés, surtout quand ces données sont utilisées à des fins policières. La loi interne doit notamment garantir que ces données soient pertinentes et non excessives au regard des finalités pour lesquelles elles sont conservées, et conservées dans une forme qui permette l'identification des personnes concernées pour une durée qui n'excède pas celle qui est nécessaire pour réaliser la finalité pour laquelle elles sont conservées. La loi interne doit offrir des protections adéquates afin que les données ainsi conservées soient efficacement protégées contre les usages non autorisés et les abus. Ces considérations sont particulièrement valables en ce qui concerne la protection des catégories particulières de données plus sensibles et plus spécialement l'information ADN qui contient la constitution génétique de l'individu qui est de grande importance pour l'individu concerné et sa famille[61].

16. La protection contre les caméras cachées

Une jeune enfant de quatorze ans avait découvert que son beau-père avait installé une caméra dans le but de la filmer lorsqu'elle prenait sa douche dans la salle de bains. Ce dernier a été, *in fine*, acquitté par les juridictions suédoises. Devant la Cour, la jeune fille s'est plainte d'une violation de son droit au respect de la vie privée. La chambre de la 5e section de la Cour a rappelé que les États devaient posséder et mettre réellement en œuvre un cadre juridique approprié qui offre

[59] En ce sens, Cour eur. D.H., arrêt *Bernh Larsen Holding AS et autres c. Norvège*, 14 mars 2013, req. no 24117/08, § 132.
[60] Cour eur. D.H., décision *Peruzzo c. Allemagne et Martens c. Allemagne*, 4 juin 2013, req. nos 7841/08 et 57900/12, § 33.
[61] *Idem*, § 42.

une protection contre les actes de violence commis par des particuliers[62] et que si le recours au droit pénal n'est pas nécessairement l'unique solution, la dissuasion effective contre des actes graves à propos de valeurs fondamentales et d'aspects essentiels de la vie privée requiert des dispositions efficaces de droit pénal[63].

En ce qui concerne des enfants, la Grande Chambre a indiqué que les dispositifs mis en place par l'État pour les protéger contre des actes de violence devaient être efficaces et inclure des mesures raisonnables visant à empêcher les mauvais traitements dont les autorités avaient ou auraient dû avoir connaissance, ainsi qu'une prévention efficace visant à mettre les enfants à l'abri de formes aussi graves d'atteinte à leur intégrité. Ces mesures doivent viser à garantir le respect de la dignité humaine et la protection de l'intérêt supérieur de l'enfant[64]. S'agissant plus spécifiquement d'actes aussi graves que le viol et les abus sexuels sur des enfants qui mettent en jeu des valeurs fondamentales et des aspects essentiels de la vie privée, il appartient aux États de se doter de dispositions pénales efficaces[65]. Concernant des actes d'une telle gravité, l'obligation positive qui incombe à l'État peut s'étendre aux questions touchant à l'effectivité d'une enquête pénale et à la possibilité d'obtenir redressement et réparation, même s'il n'existe pas un droit absolu à obtenir l'ouverture de poursuites contre une personne donnée, ou la condamnation de celle-ci, lorsqu'il n'y a pas eu de défaillances blâmables dans les efforts déployés pour obliger les auteurs d'infractions pénales à rendre des comptes[66].

Pour les actes qui pourraient passer pour présenter une gravité moins élevée, une protection pratique et efficace suppose l'existence de recours permettant d'identifier l'auteur des actes incriminés et de le traduire en justice[67]. Pour ce qui est plus généralement des actes interindividuels de moindre gravité, l'obligation qui incombe à l'État de mettre en place et d'appliquer concrètement un cadre juridique adapté n'implique pas toujours l'adoption de dispositions pénales visant les différents actes pouvant être en cause. Le cadre juridique peut aussi consister en des recours civils aptes à fournir une protection suffisante[68].

Dans l'affaire *E.S. c. Suède*, la chambre de la 5e section de la Cour avait souligné le fait qu'une vigilance croissante était nécessaire pour protéger la vie privée en présence de nouvelles technologies de la communication qui rendent possible l'enregistrement et la diffusion de données à caractère personnel[69].

---

[62] Cour eur. D.H., arrêt *E.S. c. Suède*, 21 juin 2012, req. nº 5786/08, § 58. Ce point fut repris par l'arrêt rendu en grande chambre le 12 novembre 2013, *Soderman c. Suède*, req. nº 5786/08, § 80.
[63] Cour eur. D.H., arrêt *E.S. c. Suède*, 21 juin 2012, req. nº 5786/08, § 58.
[64] Cour eur. D.H. (GC), arrêt *Soderman c. Suède*, 12 novembre 2013, req. nº 5786/08, § 81.
[65] *Idem*, § 82.
[66] *Idem*, § 83.
[67] *Idem*, § 84.
[68] *Idem*, § 85. La Cour a noté que dans certaines affaires précédentes relatives à la protection de l'image d'une personne contre des abus de la part d'autrui, les recours existants dans les États membres étaient d'ordre civil, parfois combinés à des voies procédurales telles que le prononcé d'une interdiction.
[69] Cour eur. D.H., arrêt *E.S. c. Suède*, 21 juin 2012, req. nº 5786/08, § 71.

17. La collecte et la conservation de données issues du casier judiciaire

La conservation et la divulgation de données relatives à la vie privée d'un individu tombent dans le champ de l'article 8, § 1er. Il en va de même pour les informations publiques qui sont systématiques, collectées et enregistrées dans des fichiers tenus par les autorités. C'est d'autant plus vrai quand les informations concernent le passé distant d'une personne[70].

Les données relatives à la mise en garde de la requérante et contenues dans les fichiers de la police sont des données à caractère personnel et des données sensibles. Elles font partie, en outre, de son casier judiciaire. À cet égard, la Cour souligne le fait que si les données contenues dans le casier judiciaire sont, en un sens, des données publiques, leur conservation systématique dans des fichiers centraux signifie qu'elles peuvent être divulguées longtemps après quand tout le monde a vraisemblablement oublié les événements auxquels elles sont liées. Comme la condamnation ou la mise en garde s'enfonce dans le passé, elles deviennent une partie de la vie privée de la personne qui doit être respectée[71].

La Cour considère qu'il est essentiel, dans le contexte de l'enregistrement et de la divulgation de données du casier judiciaire comme pour les écoutes téléphoniques, les surveillances secrètes et la collecte secrète d'informations, d'avoir des règles claires et détaillées qui gouvernent la portée et la mise en œuvre des mesures. Il faut aussi un minimum de règles concernant, notamment, la durée, la conservation, l'utilisation, l'accès par des tiers, les procédures de destruction, afin de fournir des garanties suffisantes contre le risque d'abus et d'arbitraire. Il y a de nombreuses étapes au cours desquelles des problèmes de protection de données peuvent surgir au regard de l'article 8, en ce compris lors de la collecte, la conservation, l'utilisation et la communication des données. À chaque étape, des protections adéquates et appropriées doivent exister et qui reflètent les principes élaborés dans les instruments applicables en matière de protection des données et empêcher l'arbitraire et les ingérences disproportionnées dans les droits garantis par l'article 8[72].

La collecte indiscriminée et illimitée dans le casier judiciaire peut difficilement être conforme avec les exigences de l'article 8 en l'absence de règles claires et détaillées décrivant, notamment, les situations dans lesquelles des données peuvent être collectées, la durée de leur conservation, l'usage qui peut en être fait et les circonstances dans lesquelles elles peuvent être détruites[73].

---

[70] Cour eur. D.H., arrêt *M.M. c. Royaume-Uni*, 13 novembre 2012, req. no 24029/07, § 187.
[71] *Idem*, § 188.
[72] *Idem*, § 195.
[73] *Idem*, § 199.

Au plus le champ d'un système d'enregistrement est grand, et donc au plus la quantité et la sensibilité des données tenues et pouvant être divulguées sont grandes, au plus sont importantes les protections à mettre en œuvre aux différentes étapes dans les traitements ultérieurs des données. La Cour considère que l'obligation de garantir le respect de la vie privée qui pèse sur les autorités responsables de la conservation et de la divulgation des données du casier judiciaire est particulièrement importante considérant la nature des données détenues et des conséquences potentiellement dévastatrices de leur divulgation[74]. La Cour est d'accord sur le fait que dans la plupart des cas, un certificat défavorable du casier judiciaire aura un effet dévastateur sur les chances d'une personne qui souhaite postuler à un emploi qui requiert sa production[75]. C'est au regard de cet effet que doit être évaluée la légalité des mesures en matière de conservation et de divulgation des données du casier judiciaire[76].

En l'absence d'un cadre juridique clair sur la collecte et la conservation de données, de l'absence de clarté sur le champ d'application, les limites et les restrictions sur les pouvoirs conférés par la loi à la police en matière de conservation et de divulgation des données relatives à la caution de la personne concernée, en l'absence de tout mécanisme de supervision indépendante des décisions de conservation ou de divulgation des données, et, en matière de divulgation des données, l'absence de distinction sur base de la nature de l'infraction, l'issue donnée à l'affaire, le temps qui s'est écoulé depuis l'infraction ou la pertinence des données par rapport à l'emploi auquel la personne postule, il ne peut pas être considéré qu'il y ait des protections suffisantes dans le système d'enregistrement et de divulgation des données du casier judiciaire qui permettent de garantir que les données relatives à la vie privée de la personne concernée n'ont pas été et ne seront pas divulguées en violation de son droit au respect de la vie privée[77].

18. La protection de l'adresse d'une personne

Une comédienne turque se plaignait d'une atteinte à sa vie privée suite à la divulgation de son adresse dans un article de presse relatant le cambriolage dont elle avait été victime. La Cour a indiqué que le choix du lieu de la résidence d'un individu était une décision essentiellement privée et que le libre exercice de ce choix faisait partie intégrante de la sphère d'autonomie personnelle protégée par l'article 8. L'adresse du domicile d'une personne constitue en ce sens une donnée ou un renseignement d'ordre personnel qui relève de la vie privée et bénéficie, à ce titre, de la protection accordée à celle-ci[78]. La Cour a rappelé que si une personne privée inconnue du public pouvait prétendre à une protection particulière de son droit à la vie privée, il n'en allait pas de même des personnes publiques qui

[74] *Idem*, § 200.
[75] *Idem*, § 200.
[76] *Idem*, § 201.
[77] *Idem*, §§ 206-207.
[78] Cour eur. D.H., arrêt *Alkaya c. Turquie*, 9 octobre 2012, req. n° 42811/06, § 30.

pouvaient néanmoins, dans certaines circonstances, se prévaloir d'une attente légitime de protection et de respect de sa vie privée[79]. Lors de la mise en balance de la protection de la vie privée et de la liberté d'expression, il faut tenir compte de l'apport de l'information publiée à un débat d'intérêt général, de la gravité de l'intrusion dans la vie privée et des répercussions de la publication pour la personne concernée[80]. À cet égard, s'il existe un droit du public à être informé qui est essentiel dans une société démocratique et qui, dans des circonstances particulières, peut même porter sur des aspects de la vie privée de personnes publiques, des publications ayant eu pour seul objet de satisfaire la curiosité d'un certain public sur les détails de la vie privée d'une personne, quelle que soit la notoriété de celle-ci, ne sauraient passer pour contribuer à un quelconque débat d'intérêt général pour la société[81]. En l'espèce, la Cour n'a pas aperçu l'intérêt général qui aurait pu justifier la divulgation par le journal de l'adresse du domicile de la requérante sans son accord[82].

19. La protection de la réputation

Le droit d'une personne à la protection de sa réputation est couvert par l'article 8 en tant qu'élément du droit au respect de la vie privée[83]. L'attaque contre la réputation personnelle doit atteindre un certain seuil de gravité et avoir été effectuée de manière à causer un préjudice à la jouissance personnelle du droit au respect de la vie privée. Mais, on ne peut se prévaloir de l'article 8 pour se plaindre d'une atteinte à sa réputation qui résulterait de manière prévisible de ses propres actions[84], telle une infraction pénale[85].

Les autorités nationales doivent adopter les mesures nécessaires afin de garantir une protection effective du droit à la réputation[86].

20. La protection de la réputation d'une personne décédée

La Cour n'exclut pas la possibilité qu'un proche puisse avoir un intérêt moral à se prévaloir du droit au respect d'une personne décédée pourvu que l'atteinte à la

[79] *Idem*, § 31.
[80] *Idem*, § 33.
[81] *Idem*, § 35.
[82] *Idem*, § 36.
[83] Cour eur. D.H., arrêt *Axel Springer c. Allemagne*, 7 février 2012, req. n° 39954/08, § 83 ; arrêt *Rosca c. Roumanie*, 4 juin 2013, req. n° 5543/06, § 95 ; arrêt *Mater c. Turquie*, 16 juillet 2013, req. n° 54997/08, § 49 ; arrêt *Somesan et Butiuc c. Roumanie*, 19 novembre 2013, req. n° 45543/04, §§ 23-24.
[84] Cour eur. D.H., arrêt *Axel Springer c. Allemagne*, 7 février 2012, req. n° 39954/08, § 83 ; arrêt *Mater c. Turquie*, 16 juillet 2013, req. n° 54997/08, § 52. Voy. aussi l'arrêt *Popovski c. l'ancienne république yougoslave de Macédoine*, 31 octobre 2013, req. n° 12316/07, § 88, sur l'obligation positive à charge de l'État d'assurer la protection effective de la vie privée et en particulier du droit au respect de la réputation.
[85] Cour eur. D.H., arrêt *Axel Springer c. Allemagne*, 7 février 2012, req. n° 39954/08, § 83.
[86] Cour eur. D.H., arrêt *Casuneanu c. Roumanie*, 16 avril 2013, req. n° 22018/10, § 80.

réputation atteigne un certain niveau de gravité et cause un dommage à l'exercice personnel du droit au respect de la vie privée de ce proche[87].

21. La publication d'articles et de photographies dans la presse

La publication d'articles et de photographies dans la presse doit respecter un équilibre entre le droit au respect de la vie privée de la personne concernée et la liberté d'expression et il n'existe aucun rapport de subordination entre eux[88].

Les obligations positives à charge des États peuvent impliquer l'adoption de mesures destinées à garantir le respect de la vie privée même dans les relations entre les particuliers, ce qui s'applique aussi à la protection de l'image d'une personne contre les abus par des tiers[89].

22. Les archives sur l'Internet

Le risque de préjudice posé par le contenu et les communications sur l'Internet à l'exercice et à la jouissance des droits et libertés, en particulier le droit au respect de la vie privée, est plus élevé que ceux posés par la presse traditionnelle. En conséquence, les règles relatives à la communication d'informations peuvent différer entre les médias imprimés et l'Internet[90].

Les archives sur l'Internet tombent dans le champ de la protection offerte par l'article 10. À cet égard, la Cour souligne l'apport substantiel des archives sur l'Internet à la conservation et à la mise à disposition de nouvelles et d'informations. Ces archives représentent une source importante pour l'éducation et la recherche historique, notamment parce qu'elles sont facilement accessibles au public et, en général, gratuites. Si la fonction première de la presse est d'agir en qualité de « chien de garde », elle a aussi un rôle secondaire important de maintenir et de mettre à la disposition du public des archives qui contiennent des nouvelles qui ont été précédemment rapportées. Le maintien d'archives sur l'Internet est un aspect critique de ce rôle[91].

---

87 Cour eur. D.H., décision *Stepniak c. Pologne*, 5 mars 2013, req. n° 45630/06, § 37.
88 Cour eur. D.H., arrêt *Aksu c. Turquie*, 15 mars 2012, req. n^{os} 4149/04 et 41209/04, § 63. Voy. aussi l'arrêt *Wegrzynowski et Smolczewski c. Pologne*, 16 juillet 2013, req. n° 33846/07, § 56. Pour des exemples d'analyse de cet équilibre, voy. l'arrêt *Von Hannover c. Allemagne (n° 2)*, 7 février 2012, req. n^{os} 40660/08 et 60641/08 ; l'arrêt *Axel Springer c. Allemagne*, 7 février 2012, req. n° 39954/08 ; l'arrêt *Aksu c. Turquie*, 15 mars 2012, req. n^{os} 4149/04 et 41209/04 ; l'arrêt *Mitkus c. Lettonie*, 2 octobre 2012, req. n° 7259/03 ; l'arrêt *Rothe c. Autriche*, 4 décembre 2012, req. n° 6490/07 ; l'arrêt *Ageyevyv c. Russie*, 18 avril 2013, req. n° 7075/10 ; l'arrêt *Von Hannover c. Allemagne (n° 3)*, 19 septembre 2013, req. n° 8772/10 ; l'arrêt *Pauliukiene et Pauliukas c. Lituanie*, 5 novembre 2013, req. n° 18310/06 ; l'arrêt *Somesan et Butiuc c. Roumanie*, 19 novembre 2013, req. n° 45543/04 ; l'arrêt *Putistin c. Ukraine*, 21 novembre 2013, req. n° 16882/03 ; l'arrêt *Khmel c. Russie*, 12 décembre 2013, req. n° 20383/04.
89 Cour eur. D.H., arrêt *Rothe c. Autriche*, 4 décembre 2012, req. n° 6490/07, § 39.
90 Cour eur. D.H., arrêt *Wegrzynowski et Smolczewski c. Pologne*, 16 juillet 2013, req. n° 33846/07, § 58. Voy. la question de la responsabilité pour des propos diffamatoires tenus sur un portail d'actualités sur internet, l'arrêt *Delfi AS c. Estonie*, 10 octobre 2013, req. n° 64569/09, renvoyé devant la grande chambre qui ne s'est pas encore prononcée.
91 Cour eur. D.H., arrêt *Wegrzynowski et Smolczewski c. Pologne*, 16 juillet 2013, req. n° 33846/07, § 59.

La Cour a déjà considéré que l'obligation de mettre une mention appropriée sur un article contenu dans une archive sur l'Internet, quand il a été signalé au journal qu'une action en diffamation a été introduite en raison de cet article publié dans la presse écrite, ne constituait pas une ingérence disproportionnée dans la liberté d'expression[92]. Dans le même temps, la Cour avait approuvé le fait que les juridictions nationales n'avaient pas suggéré que les articles potentiellement diffamatoires soient retirés des archives[93].

23. La protection des sources journalistiques

La protection des sources journalistiques est une des pierres angulaires de la liberté de la presse[94]. Toute obligation de les divulguer est incompatible avec l'article 10 sauf à être justifiée par un impératif primordial d'intérêt public[95].

24. Les communications téléphoniques en prison

L'article 8 ne garantit pas aux prisonniers le droit de téléphoner, en particulier quand il leur est loisible de correspondre par écrit. Lorsque la prison leur offre la possibilité de téléphoner, il peut y avoir des contraintes légitimes liées, par exemple, au fait que les équipements sont partagés avec les autres prisonniers ou à la nécessité de prévenir les désordres et les infractions[96].

La présence d'un gardien lors des communications téléphoniques et l'enregistrement des numéros composés depuis la prison constituent des ingérences dans le droit des détenus au respect de leur vie privée mais justifiées dans la mesure où cette surveillance est moins intrusive que les écoutes téléphoniques et que le détenu est averti de cette surveillance[97].

Lorsqu'un courrier électronique est envoyé à la boîte à message générale de la prison mais avec l'indication qu'il est destiné à un détenu déterminé et qu'il est demandé de le lui communiquer, le détenu peut s'attendre à ce que cette correspondance soit protégée par l'article 8[98]. Il n'y a pas d'obligation positive à charge de l'État d'autoriser l'usage des e-mails[99]. Le refus de communiquer l'e-mail au détenu n'est pas non plus une mesure disproportionnée dès lors que son expéditeur avait été prévenu de la non-communication du message et avait été requis d'utiliser les moyens de communication autorisés par la législation nationale[100].

---

92 *Ibidem*.
93 *Ibidem*.
94 Cour eur. D.H., arrêt *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, 22 novembre 2012, req. nº 39315/06, § 127. Voy. aussi l'arrêt *Saint-Paul Luxembourg S.A. c. Luxembourg*, 18 avril 2013, req. nº 26419/10, § 49.
95 Cour eur. D.H., arrêt *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, 22 novembre 2012, req. nº 39315/06, § 127.
96 Cour eur. D.H., décision *Daniliuc c. Roumanie*, 2 octobre 2012, req. nº 7262/06, § 68.
97 Cour eur. D.H., arrêt *Niculescu c. Roumanie*, 25 juin 2013, req. nº 25333/03, § 92.
98 Cour eur. D.H., arrêt *Helander c. Finlande*, 10 septembre 2013, req. nº 10410/10, § 48.
99 *Idem*, § 53.
100 *Idem*, § 54.

25. Les fichiers d'enregistrement des immatriculations

La Cour a été saisie d'une affaire dans laquelle le permis du requérant lui avait été dérobé. Les voleurs ont ensuite utilisé ce permis pour enregistrer 1.737 voitures dans le registre des immatriculations. La situation a causé de très nombreux désagréments au requérant et les juridictions internes n'ont jamais accepté d'y remédier de façon suffisante. La Cour a d'abord considéré que le défaut d'invalider le permis de conduire du requérant dès que son vol avait été déclaré (ce qui a rendu possible l'abus de l'identité du requérant par des tiers), constituait une ingérence dans le droit du requérant au respect de sa vie privée. La Cour a ensuite jugé qu'il n'était pas nécessaire de se pencher sur la question de savoir si le requérant avait pris les mesures appropriées par rapport aux enregistrements abusifs de véhicules en son nom. Elle a simplement considéré que, dès le moment où le requérant avait déclaré le vol de son permis de conduire, les autorités publiques néerlandaises ne pouvaient plus prétendre ignorer que le détenteur du permis n'était pas le requérant[101].

26. Registre de faillis

L'Italie a encore fait l'objet d'une série de condamnations pour sa législation en matière d'inscription dans le registre des faillis compte tenu de la nature automatique de l'inscription, de l'absence de toute évaluation et de tout contrôle juridictionnel sur l'application des incapacités et du laps de temps prévu pour l'obtention d'une réhabilitation (soit cinq ans après la clôture de la procédure de faillite)[102].

27. L'accès aux diagnostics génétiques préimplantatoires et aux procréations médicalement assistées

Le désir de procréer un enfant qui ne soit pas atteint par la mucoviscidose et de recourir pour ce faire à la procréation médicalement assistée et au diagnostic préimplantatoire relève de la protection de l'article 8[103].

28. L'interdiction d'utiliser des embryons, la recherche scientifique et la liberté d'expression

La recherche scientifique peut être une forme de liberté de communication d'information qui profite aux chercheurs et aux scientifiques. En ce sens, l'interdiction d'utiliser des embryons pourrait dès lors constituer une ingérence à ce sujet dans leur chef[104].

---

[101] Cour eur. D.H., arrêt *Romet c. Les Pays-Bas*, 14 février 2012, req. n° 7094/06, §§ 37 et s.
[102] Cour eur. D.H., arrêt *Salvatore Coppola et autres c. Italie*, 18 décembre 2012, req. n^{os} 5179/05, 14611/05, 29701/06, 9041/05 et 8239/05, §§ 36 et s. Voy. aussi l'arrêt *De Carolis c. Italie*, 5 mars 2013, req. n° 33359/05.
[103] Cour eur. D.H., arrêt *Costa et Pavan c. Italie*, 28 août 2012, req. n° 54270/10, § 57 (comparez avec l'arrêt *S.H. c. Autriche*, 3 novembre 2011, req. n° 57813/00).
[104] Voy. la décision *Parrillo c. Italie*, 28 mai 2013, req. n° 46470/11.

Claire Gayrel, Jean Herveg et Jean-Marc Van Gyseghem

II. La Cour de justice de l'Union européenne

Nous commencerons cette chronique par les décisions faisant application des droits fondamentaux relatifs à la protection de la vie privée et des données à caractère personnel reconnus respectivement aux articles 7 et 8 de la Charte des droits fondamentaux (A). Après avoir présenté les positions des juridictions quant aux notions de traitement et de données à caractère personnel (B), nous présenterons les décisions portant sur l'interprétation de dispositions de la directive 95/46 (C), de la directive 2002/58 (D) et du règlement 45/2001 (E) pertinents pour notre chronique.

A. L'application du droit fondamental à la vie privée et à la protection des données

1. *L'invalidité de la directive relative à la conservation des données de trafic*[105]

Saisie de demandes préjudicielles introduites par la High Court (Irlande) et le Verfassungsgerichtshof (Autriche), la Cour a annulé la directive 2006/24 relative à la conservation des données de trafic[106], pour cause d'invalidité avec les droits reconnus aux articles 7 et 8 de la Charte. Pour rappel, la directive 2006/24 avait pour objectif d'harmoniser les dispositions nationales relatives à la conservation, pour une durée de six mois à deux ans, par les fournisseurs de services de communications accessibles au public ou de réseaux publics de communications, de l'ensemble des données de trafic (mobile, fixe, téléphonie par internet, et internet), en vue de garantir leur disponibilité à des fins de prévention, recherche, détection et poursuite d'infractions graves. Cette annulation intervient huit ans après l'adoption de la directive, alors que les lois nationales de transposition avaient déjà suscité un contentieux national important. Il est notable que l'effet de cette annulation vaut *ab initio*, entraînant aussi le remboursement de l'amende payée par la Suède suite à sa condamnation pour transposition tardive de la directive[107]. Toutefois, l'arrêt de la Cour ne vaut que pour le droit de l'Union et laisse intactes les mesures de droit national existantes[108].

La pertinence des articles 7 et 8 de la Charte est établie par la Cour en raison du fait que les données de trafic « prises dans leur ensemble, sont susceptibles

[105] C.J. (GC), 8 avril 2014, *Digital Rights Ireland*, aff. C-293/12. Pour plus d'informations, voy. E. Guild et S. Carrera, « The Political and Judicial Life of Metadata : *Digital Rights Ireland* and the Trail of the Data Retention Directive », *CEPS Paper for Liberty & Security*, n° 65, mai 2014 ; I. Chatelier et M.-V. Perez Asinari, « Arrêt *Digital Rights Ireland* : invalidité de la directive sur la conservation des données de trafic », *J.D.E.*, 2014, pp. 250-252.

[106] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.* L 105, 13 avril 2006.

[107] C.J., 30 mai 2013, *Commission c. Suède*, aff. C-270/11.

[108] Pour plus d'informations sur les conséquences de l'arrêt *Digital Rights Ireland* sur les mesures nationales de transposition, voy. notamment A. Wiedman, « Le dialogue sur les droits fondamentaux entre la Cour de justice et les juridictions nationales après l'arrêt *Digital Rights Ireland et Seitlinger e.a.* », *R.A.E.*, n° 2, 2014, pp. 423-432 et F. Boehm et M. D. Cole, « Data Retention After the Judgement of the Court of Justice of the European Union », 30 juin 2014, Rapport commandé par le député européen J.-P. Albreicht.

de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées ...»[109]. La Cour distingue ensuite l'ingérence occasionnée par la conservation des données, de l'ingérence occasionnée par l'accès auxdites données de trafic[110]. Si le contenu essentiel des droits fondamentaux protégés aux articles 7 et 8 de la Charte n'est pas atteint[111], elle considère qu'eu égard à l'ampleur et à la gravité de l'ingérence, la Cour est appelée à exercer un contrôle de légalité strict[112]. Dans son analyse de proportionnalité, la Cour va d'abord considérer, sans surprise, que la mesure remplit la condition d'appropriation, en ce sens que la conservation des données de trafic peut être considérée comme apte à contribuer à l'élucidation d'infractions graves[113]. En revanche, la Cour va juger que la mesure ne saurait être considérée comme limitée au strict nécessaire. Trois arguments principaux sont développés. En premier lieu, la Cour soulève le problème de la rétention globale, sans distinction, différentiation, ni exception des données de trafic[114]. En particulier, sont visées ici la conservation de données relatives à des personnes pour lesquelles « il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves », l'absence d'exceptions pour les personnes soumises au secret professionnel, mais aussi l'absence de limites temporelles, géographiques ou personnelles à cette conservation, et par là l'absence d'exigence d'une relation entre les données à conserver et une menace spécifique à la sécurité publique. En deuxième lieu, la Cour considère que la directive ne prévoit aucun critère objectif délimitant l'accès des autorités nationales compétentes[115]. Ici la Cour juge insatisfaisant le renvoi au droit national, considérant que c'était au législateur européen lui-même de prévoir les garanties, et notamment procédurales, organisant l'accès et l'utilisation des données. Enfin, la Cour critique la durée de conservation, dont la nécessité n'est pas suffisamment établie[116].

2. *La validité du passeport biométrique européen*

La Cour a eu à examiner la validité du passeport biométrique européen, contenant une photo faciale et deux empreintes digitales[117]. Reconnaissant que le prélèvement et la conservation d'empreintes digitales par les autorités nationales constituent une atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel, la Cour a ensuite considéré que cette mesure était proportionnée aux buts poursuivis, à savoir prévenir la falsification des passeports et empêcher leur utilisation frauduleuse[118]. Après avoir discuté les

[109] Affaire *Digital Rights Ireland*, point 27.
[110] *Idem*, points 34 et 35.
[111] *Idem*, points 39 et 40.
[112] *Idem*, point 48.
[113] Points 49 et 50.
[114] Points 57 à 59.
[115] Points 60 à 62.
[116] Points 63 et 64.
[117] En particulier article 1er, paragraphe 2, du règlement 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, *J.O.C.E.* L 385 du 29 décembre 2004.
[118] C.J., 17 octobre 2013, *Michael Schwarz c. Stadt Bochum*, aff. C-291/12.

alternatives disponibles telle que la reconnaissance de l'iris, la Cour a finalement admis qu'il n'avait pas été porté à sa connaissance l'existence de mesures alternatives susceptibles de contribuer, de manière suffisamment efficace, aux buts poursuivis[119]. Dans ce cadre, le prélèvement d'empreintes digitales doit être considéré comme valide. Enfin, concernant l'argument soulevé tenant au risque d'utilisation ultérieure des empreintes digitales qui seraient conservées de manière centralisée par les États membres à d'autres fins, la Cour affirme que la validité de telles mesures devrait être examinée par les juridictions nationales, puisque le règlement ne prévoit pas de conservation centralisée des empreintes[120].

B. Notions de données à caractère personnel, de traitement et de responsable de traitement

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. L'examen fait par les juridictions de ces notions est en effet essentiel pour déterminer le champ d'application matériel des textes et donc, de l'étendue de la protection qu'ils confèrent.

La Cour de justice a constaté que les données figurant dans un registre du temps de travail concernant, pour chaque travailleur, les périodes de travail et de repos constituaient des données à caractère personnel et que leur collecte, enregistrement, organisation, consultation, utilisation et transmission étaient un traitement de données[121]. Dans une autre affaire, la Cour a évidemment reconnu que la collecte, conservation et transmission de données portant sur des personnes physiques par des détectives privés constituaient un traitement[122]. Le Tribunal a quant à lui précisé que l'information permettant d'identifier personnellement les auteurs de certaines observations, en l'espèce l'information reliant chaque observation à l'expert qui l'a émise, constituait des données à caractère personnel[123].

Dans le cas des activités des moteurs de recherche[124], la Cour a observé que «les données trouvées, indexées, stockées par les moteurs de recherche et mises à la disposition de leurs utilisateurs» concernent pour partie des données à caractère personnel et que les activités d'exploration automatisée, constante et systématique d'Internet à la recherche des informations qui y sont publiées par l'exploitant d'un moteur de recherche en vue de leur collecte, de leur enregistrement sur ses serveurs, de leur

119 *Idem*, point 53.
120 *Idem*, point 62.
121 C.J., 30 mai 2013, *Worten*, aff. C-342/12, points 19 et 20 ; C.J., 19 juin 2014, *Pharmacontinente – Saude e Higiene SA*, aff. C-683/13, point 12.
122 C.J., 7 novembre 2013, *Institut Professionnel des agents immobiliers (IPI)*, aff. C-473/12, point 26.
123 Trib., 13 septembre 2013, *ClientEarth & Pesticide Action Network Europe (PAN Europe) c. Autorité européenne de sécurité alimentaire (EFSA)*, aff. T-214/11, point 46.
124 C.J. (GC), 13 mai 2014, *Google Spain SL c. Mario Costeja Gonzalès*, aff. C-131/12.

organisation au moyen d'un programme d'indexation et enfin de leur communication aux utilisateurs constituent indubitablement des traitements de données visés à l'article 2, b), de la directive 95/46. Plus discutée était la question de savoir si Google était « responsable de traitement », alors que cette dernière n'a pas de contrôle sur les données publiées sur les pages web de tiers. Pour la Cour, « le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue de et s'ajoute à celui effectué par les éditeurs de sites web, consistant à faire figurer ces données sur une page Internet »[125]. Pour la Cour, les moteurs de recherche jouent un rôle décisif dans la diffusion globale desdites données[126] et leurs activités sont donc susceptibles « d'affecter significativement et de manière inconditionnelle par rapport à celle des éditeurs de sites web les droits fondamentaux de la vie privée et de la protection des données à caractère personnel »[127]. Dans ce cadre, pour que les garanties apportées par la directive 95/46 puissent développer leur plein effet, il revient à l'exploitant d'un moteur de recherche en tant que personnel déterminant les finalités et les moyens de cette activité et « dans le cadre de ses responsabilités, de ses compétences et ses possibilités » d'assurer le respect de la directive 95/46[128].

Dans une décision rendue par le TFP, la notion de données à caractère personnel a en revanche été mal appliquée. Le TFP était saisi d'un recours, visant à annuler la décision du jury de l'EPSO[129] de ne pas l'inscrire sur la liste des lauréats à un concours[130]. Le requérant soutenait, entre autres, qu'EPSO aurait violé son obligation de motivation en refusant de lui communiquer plusieurs documents, en particulier sa copie corrigée, les raisons pour lesquelles il avait échoué ainsi que les grilles d'évaluation utilisées. Le Tribunal a pour sa part considéré que de tels documents étaient couverts par le secret du jury, rejetant les arguments tirés d'une violation de l'article 8 de la Charte et du règlement 45/2001. En effet, pour ce dernier « par données personnelles sont uniquement visées les informations susceptibles de permettre l'identification d'une personne. Il s'ensuit qu'en vertu des dispositions précitées, le requérant est en droit d'obtenir un accès aux données détenues par l'EPSO permettant de l'identifier et non un accès à sa copie corrigée, aux questions sur lesquelles il a échoué, aux raisons pour lesquelles ses réponses étaient erronées ou à la grille d'évaluation utilisée. Il en est d'autant plus ainsi que, s'il devait être considéré que la copie corrigée d'un candidat constitue une donnée personnelle, ce dernier pourrait, conformément à l'article 14 du règlement n° 45/2001, demander à ce que celle-ci soit rectifiée, ce qui serait absurde »[131]. Le TFP a commis une erreur manifeste d'interprétation, puisque la copie corrigée d'un candidat à un examen, ainsi que la grille d'évaluation, constituent de toute évidence des données à caractère personnel relatives à la personne candidate à un examen. Pour autant, le candidat ne dispose pas nécessairement d'un droit de rectification,

[125] Point 35.
[126] Point 36.
[127] Point 38.
[128] *Idem*.
[129] European Personnel Selection Office.
[130] TFP, 12 février 2014, *Gonzalo de Mendoza Asensi c. Commission européenne*, aff. F-127/11.
[131] *Idem*, point 101.

qui n'est octroyé que pour des « données incomplètes ou inexactes »[132]. Il aurait été parfaitement possible pour le juge d'expliquer que le droit de rectification ne pouvait être valablement invoqué dans le cas d'une copie d'examen pour modifier une réponse indiquée comme insuffisante ou erronée par l'évaluateur.

C. Directive 95/46 « protection des données à caractère personnel »

1. *Champ d'application territorial*

Dans l'affaire *Google Spain*, il s'agissait de déterminer si l'activité d'indexation, bien que réalisée par Google Search, dont le siège se situe en dehors du territoire de l'Union, tombait ou non dans le champ d'application territorial de la directive 95/46. En effet, c'est la filiale Google Spain dont les activités se limitent à la promotion et la vente de produits et services de publicité en ligne en Espagne qui se trouvait en cause, alors même que l'activité d'indexation, et donc le traitement de données à caractère personnel caractérisé plus tôt par la Cour (voy. *supra*), n'était pas réalisé par Google Spain. La Cour a rappelé que la directive 95/46 vise à s'appliquer aux traitements de données à caractère personnel effectués « dans le cadre » des activités d'un établissement du responsable de traitement sur le territoire d'un État membre, et pas seulement aux traitements effectués « par » cet établissement[133]. En l'espèce, la Cour considère que « les activités de l'exploitant du moteur de recherche et celles de son établissement situé dans l'État membre concerné sont indissociablement liées dès lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités »[134]. Dès lors, la Cour a jugé que « l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires par ce moteur et dont l'activité vise les habitants de cet État membre »[135].

2. *Légitimité*

Dans les affaires *Worten*[136] et *Pharmacontinente*[137], la Cour a jugé qu'une réglementation nationale qui impose à l'employeur l'obligation de mettre à la disposition de l'autorité nationale compétente en matière de surveillance des conditions de travail

[132] Article 14 du règlement 45/2001.
[133] Affaire *Google Spain*, point 52.
[134] *Idem*, point 56.
[135] *Idem*, point 60.
[136] Affaire *Worten*, point 45.
[137] Affaire *Pharmacontinente*, point 12.

le registre du temps de travail afin d'en permettre la consultation immédiate, pour autant que cette mesure soit jugée nécessaire pour une application plus efficace de la réglementation, est compatible avec la directive 95/46 et notamment son article 7, sous c) et e) autorisant les traitements de données « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis » ou « à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ».

3. *Portée des exceptions prévues à l'article 13*

Dans le cadre d'un renvoi préjudiciel portant sur l'étendue des exceptions prévues à l'article 13 de la directive, la Cour a rappelé que les États membres disposaient d'une faculté et non d'une obligation de prévoir des exceptions pour les cas visés à l'article 13[138]. Dans le cas qui lui était soumis, la Cour a jugé que « l'activité de détective privé agissant pour un organisme professionnel afin de rechercher des manquements à la déontologie d'une profession réglementée, en l'occurrence celle d'agent immobilier » relevait bien de l'exception prévue à l'article 13, paragraphe 1, sous d)[139].

4. *Principe de sécurité*

Dans l'affaire *Worten* relative à l'accès aux registres du temps de travail par l'autorité nationale du contrôle des conditions de travail, la Cour a jugé qu'il incombe à tout responsable de traitement, conformément à l'article 17, § 1er, de la directive, « d'adopter les mesures techniques et d'organisation nécessaires pour s'assurer que seules des personnes dûment autorisées à accéder aux données à caractère personnel concernées soient en droit de répondre à une demande d'accès émanant d'un tiers »[140].

5. *Droit d'accès*

La Cour a jugé que l'article 12 sous a) relatif au droit d'accès des individus aux données à caractère personnel les concernant, ne s'opposait pas à la perception de frais, tel qu'un droit de timbre, pour la communication par une autorité publique de données à caractère personnel[141]. Il appartient aux États membres de fixer le montant desdits frais « à un niveau qui constitue un juste équilibre entre d'une part, l'intérêt de la personne concernée à protéger sa vie privée, et [...], d'autre part, la charge que l'obligation de communiquer ces informations représente pour le responsable de traitement »[142]. Toutefois, pour que de tels frais ne soient pas susceptibles de constituer un obstacle à l'exercice du droit d'accès, la Cour indique que « leur montant ne doit pas excéder le coût de la communication de ces données »[143].

---

138 Affaire *IPI*, point 48.
139 *Idem*, point 53.
140 Affaire *Worten*, point 28.
141 C.J., 12 décembre 2013, *X* (renvoi préjudiciel par le Gerechtshof te's-Hertogenbosch (Pays-Bas), aff. C-486/12.
142 *Idem*, point 28.
143 *Idem*, point 31.

6. *Droit d'effacement, d'opposition et droit à l'« oubli »*[144]

Après avoir considéré que Google était bien responsable d'un traitement de données à caractère personnel entrant dans le champ d'application de la directive, la Cour devait déterminer si le requérant pouvait solliciter la suppression, par Google, d'un lien de la liste de résultats affichée à partir d'une recherche effectuée sur base de son nom. Tandis que l'avocat général avait considéré que cette obligation de suppression ne valait qu'à titre subsidiaire, c'est-à-dire après que la personne concernée eut d'abord exercé son droit d'effacement auprès de l'éditeur de la page web sur laquelle figureraient les informations à supprimer, la Cour a quant à elle rejeté une telle approche. Selon elle, « compte tenu de la facilité avec laquelle des informations publiées sur un site web peuvent être répliquées [...], une protection efficace et complète ne pourrait être réalisée si celles-ci devaient d'abord ou en parallèle obtenir l'effacement des informations les concernant auprès des éditeurs de site web »[145].

Quant à la portée des droits protégés par l'article 12, sous b) (droit d'effacement « en raison du caractère incomplet ou inexact des données ») ou à l'article 14, alinéa 1er, sous a) (droit d'opposition), la Cour ira même plus loin, en considérant que « même un traitement initialement licite de données exactes, peut devenir, avec le temps, incompatible avec cette directive, [...] Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard [des finalités initiales du traitement] et du temps qui s'est écoulé ». Dès lors, même le lien d'une information exacte et publiée de manière licite peut perdre sa « pertinence » avec le temps et donc faire l'objet d'une demande d'effacement. Pour la Cour, il n'est pas nécessaire que l'information en question apparaissant dans la liste de résultats cause un préjudice à la personne concernée, cette dernière « pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats ». Si de tels droits « prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne », l'équilibre entre vie privée et droit d'accès à l'information devra être recherché en fonction de « la nature de l'information en question, de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique »[146].

---

[144] Voy. notamment C. de Terwangne, « Droit à l'oubli ou droit à l'autodétermination informationnelle », in D. Dechenaud (coord.), *Le droit à l'oubli*, Recherche effectuée pour la Mission Droit et Justice, Bruxelles, Larcier, 2014, pp. 12-34 ; E. Defreyne et R. Robert, « L'arrêt 'Google Spain' : une clarification de la responsabilité des moteurs de recherche… aux conséquences encore floues », note sous C.J.U.E. (GC), 13 mai 2014, *R.D.T.I.*, n° 56, 2015.

[145] *Google Spain*, point 84.

[146] *Idem*, point 81. Pour une critique de la décision de la Cour au regard du droit d'accès à l'information, voy. Q. Van Enis, « Le droit de recevoir des informations ou des idées par le biais d'Internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen ? », *J.E.D.H.*, à paraître 2015.

7. *Indépendance des autorités de contrôle*

Réunie en Grande Chambre, la Cour était saisie de deux requêtes de la Commission européenne contre l'Autriche et la Hongrie visant à établir le manquement de ces deux États à leurs obligations au titre de l'article 28 de la directive 95/46 relatif à l'indépendance des autorités de contrôle[147]. Ce n'est pas la première fois que la Cour de justice est amenée à préciser les garanties d'indépendance attendues pour une autorité nationale de protection des données. Pour rappel, la Cour a déjà jugé que l'Allemagne avait manqué à son obligation en soumettant les autorités de contrôle du secteur non public à la tutelle de l'État[148].

Dans le cas de l'Autriche, trois questions principales ont été soulevées. En premier lieu, il s'agissait de déterminer si une tutelle de service restreinte, telle que prévue par la loi de 1979 relative au statut des fonctionnaires et à laquelle le membre administrateur de la Datenschutzkommission (ci-après DSK, autorité autrichienne de protection des données) est soumis, pouvait être constitutive d'une influence extérieure indirecte, et donc incompatible avec l'objectif d'exercer ses missions « en toute indépendance ». Contre les arguments de l'Autriche, et de l'Allemagne pour lesquels une tutelle de service restreinte est conforme à l'article 28, § 1er, de la directive 95/46, mais aussi à la condition d'indépendance inhérente à l'article 267 TFUE, la Cour a considéré que si l'indépendance fonctionnelle, entendu en ce sens que les membres ne sont liés par aucune instruction dans l'exercice de leur fonction, constitue certes une condition nécessaire, elle n'en constitue pas une condition à elle seule suffisante pour préserver ladite autorité de toute influence extérieure[149]. En l'espèce, dans la mesure où le membre administrateur du DSK est un fonctionnaire fédéral issu de la Chancellerie, ses liens de service avec cet organe politique ne permettent pas d'affirmer que la DSK soit au-dessus de tout soupçon de partialité[150]. En deuxième lieu, la Cour a considéré que l'intégration du bureau de la DSK aux services de la Chancellerie fédérale, et notamment le fait que le personnel du bureau du DSK soit composé de fonctionnaires de la Chancellerie fédérale, n'était pas compatible avec l'exigence d'indépendance prévue à l'article 28[151]. Enfin, la Cour a jugé que le droit à l'information très vaste et inconditionnel dont bénéficie le chancelier fédéral auprès du président et du membre administrateur de la DSK prévu par la loi nationale de protection des données ne saurait garantir que la DSK exerce « en toute indépendance » les missions dont elle est investie[152].

La Cour a jugé qu'en mettant fin anticipativement au mandat de l'autorité nationale de contrôle de la protection des données, à la suite d'un changement de modèle institutionnel décidé par la loi, la Hongrie avait violé ses obligations au titre de l'article 28, § 1er, alinéa 2, de la directive 95/46, « laquelle implique

147 C.J. (GC), 16 octobre 2012, *Commission c. Autriche*, aff. C-614/10.
148 C.J. (GC), 9 mars 2010, *Commission c. Allemagne*, aff. C-518/07.
149 Affaire *Commission c. Autriche*, § 42.
150 *Idem*, § 52.
151 *Idem*, § 59.
152 *Idem*, §§ 63 et 64.

l'obligation de respecter la durée du mandat de celle-ci »[153]. Pour la Cour, « s'il était loisible à chaque État membre de mettre fin au mandat d'une autorité de contrôle avant le terme initialement prévu de celui-ci sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, la menace d'une telle cessation anticipée qui planerait alors sur cette autorité ... pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique, incompatible avec ladite exigence d'indépendance »[154].

D. Directive 2002/58 « vie privée et communications électronique »

1. *Limitations à la confidentialité des communications pour la poursuite des infractions aux droits d'auteur*

La Cour a eu l'occasion de confirmer dans l'affaire *Bonnier*[155] sa jurisprudence bien établie depuis l'affaire *Promusicae*[156] selon laquelle « le droit communautaire, notamment l'article 8, paragraphe 3, de la directive 2004/48[157], lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58, ne s'oppose pas à ce que les États membres établissent une obligation de transmission à des personnes privées tierces de données à caractère personnel relatives au trafic pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur »[158]. Comme dans l'affaire *Promusicae*, la Cour rappelle que c'est aux États membres d'établir le juste équilibre entre confidentialité des communications d'un côté et protection des droits d'auteur de l'autre. En l'espèce, la Cour a toutefois souligné que la législation suédoise en cause devait être considérée, en principe, comme assurant un juste équilibre puisque qu'elle prévoit que l'injonction judiciaire de communiquer les données d'identification relative à l'abonné ne puisse être ordonnée que si des indices réels d'atteinte à un droit de propriété intellectuelle sur une œuvre existent[159]. Cette condition serait satisfaisante car elle permettrait au juge « de pondérer, en fonction des circonstances de chaque espèce et en tenant dûment compte des exigences résultant du principe de proportionnalité, les intérêts opposés en présence »[160].

---

153 C.J. (GC), 8 avril 2014, *Commission européenne c. Hongrie*, aff. C-288/12, point 60.
154 *Idem*, point 45.
155 C.J., 19 avril 2012, *Bonnier Audio AB*, aff. C-461/10.
156 C.J.C.E. (GC), 29 janvier 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, aff. C-275/06.
157 Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, *J.O.U.E.* L 195, 2 juin 2004.
158 Affaire *Bonnier*, point 55. Voy. aussi C.J.C.E., 19 février 2009, *LSG-Gesellschaft c. Tele2 Telecommunication GmbH*, aff. C-557/07, point 29 et C.J.C.E, aff. *Promusicae*, point 70.
159 Affaire *Bonnier*, point 58.
160 *Idem*, point 59.

2. *Exception à la confidentialité des communications pour les finalités de facturation*

Dans l'affaire *Probst*, la Cour devait préciser les conditions prévues pour la transmission de données de trafic par un fournisseur de services à un tiers, en l'espèce le cessionnaire de ses créances, telles que prévues par l'article 6, §§ 2 et 5 de la directive 2002/58[161]. Tout d'abord la Cour a considéré que cette disposition autorise le traitement de données relatives au trafic, « non seulement aux fins de l'établissement des factures, mais également aux fins de leur recouvrement »[162]. En deuxième lieu, la Cour a jugé que si l'article 6, §§ 2 et 5 contient une exception à la confidentialité des communications prévue à son article 5, § 1er, en prévoyant la possibilité pour le fournisseur de service de sous-traiter à des tiers les missions de facturation et de recouvrement des créances, le transfert des données de trafic à ces fins devait être restreint aux personnes agissant « sous l'autorité » du fournisseur de services, cette disposition appelant une interprétation stricte[163]. Dans ce cadre, et suivant une lecture combinée des dispositions de la directive 2002/58 et des articles 16 et 17 de la directive 95/46 relatifs au recours à des sous-traitants pour le traitement de données à caractère personnel, la Cour a considéré que l'objectif de l'article 6, § 5 visait bien à ce « qu'une telle externalisation n'affecte pas le niveau de protection des données »[164]. En l'espèce, il revient à la juridiction nationale de vérifier que le contrat conclu entre le fournisseur de services et le cessionnaire de créances comporte les dispositions nécessaires de nature à garantir la licéité du traitement des données de trafic.

E. Règlement 45/2001 sur la protection des données personnelles traitées par les institutions et droit d'accès aux documents des institutions

Le Tribunal a eu à poursuivre l'application de la jurisprudence *Bavarian Lager*[165] relative à l'articulation des règlements 45/2001 et 1049/2001[166] posée par l'article 4, § 1er, sous b)[167] de ce dernier quant à l'équilibre entre la protection de la vie privée et des données à caractère personnel d'un côté et la transparence administrative de l'autre. Il a notamment précisé dans deux décisions contrastées les obligations de motivation s'appliquant aux institutions refusant l'accès sur le fondement de l'exception prévue à l'article 4, § 1er, sous b), du règlement 1049/2001, et celles s'appliquant au demandeur sollicitant l'accès à des documents couverts par cette exception.

---

161 C.J., 22 novembre 2012, *Josef Probst c. mr.nexnet GmbH*, aff. C-119/12.
162 *Idem*, point 17.
163 *Idem*, point 23.
164 *Idem*, point 26.
165 C.J. (GC), 29 juin 2010, *Commission c. The Bavarian Lager Co. Ltd*, aff. C-28/08.
166 Règlement nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, *J.O.C.E.* L 145, 31 mai 2001.
167 « Les institutions refusent l'accès à un document dans le cas où la divulgation porterait atteinte à la protection : [...] b) de la vie privée et de l'intégrité de l'individu, notamment en conformité avec la législation communautaire relative à la protection des données à caractère personnel ».

Dans le premier cas, c'est au Parlement européen que le Tribunal a reproché l'absence de motivation pour refuser l'accès à des documents sur la base de l'exception prévue à l'article 4, § 1er, sous b). Conformément à une jurisprudence constante selon laquelle « les exceptions à l'accès aux documents doivent être interprétées et appliquées de manière stricte »[168], « une simple affirmation selon laquelle l'accès à certains documents porterait atteinte à la vie privée » n'est pas valable[169]. En effet, il incombe à l'institution de procéder à un examen concret, et de démontrer dans chaque cas d'espèce, sur la base des informations dont elle dispose, que la divulgation des documents auxquels l'accès est sollicité porterait concrètement et effectivement atteinte à la vie privée des personnes concernées[170], le risque d'atteinte devant être raisonnablement prévisible et non purement hypothétique[171].

Dans le second cas, le Tribunal a confirmé que la demande d'accès à des documents administratifs contenant des données à caractère personnel couverts par l'exception de l'article 4, § 1er, sous b), du règlement 1049/20001 devait alors satisfaire les exigences prévues par l'article 8, sous b)[172] du règlement 45/2001[173]. Interprétant cette disposition, le Tribunal considère qu'il revient au demandeur destinataire de démontrer dans sa demande la nécessité du transfert, ainsi que le fait qu'il n'existe aucune raison légitime que ce transfert puisse porter atteinte aux intérêts légitimes des personnes concernées, ces deux conditions étant cumulatives[174]. Pour le Tribunal, les demandeurs n'auraient pas suffisamment démontré que le transfert des données qu'ils demandaient était nécessaire en l'espèce.

Claire Gayrel

Chercheuse senior au Centre de Recherches Information, Droit et Société (www.crids.eu)
Auteure de la partie consacrée aux juridictions de l'Union européenne

Jean Herveg

Directeur de Recherche au Centre de Recherches Information, Droit et Société (www.crids.eu),
avocat au barreau de Bruxelles (www.rawlingsgiles.be)
Auteur de la partie consacrée à la Cour européenne des droits de l'homme

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)
Coordinateur de la contribution

168 Trib., 28 mars 2012, *Kathleen Egan et Margaret Hackett c. Parlement européen*, aff. T-190/10, point 88.
169 *Idem*, point 91.
170 *Idem*, points 90, 93, 101.
171 *Idem*, point 93.
172 « les données à caractère personnel ne sont transférées à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE que si a) [...] b) le destinataire démontre la nécessité de leur transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes de la personne concernée ».
173 Affaire *ClientEarth & autres c. AESA*, point 64.
174 *Idem*, point 83.