La protection des données à caractère personnel en droit européen

Herveg, Jean; Van Gyseghem, Jean-Marc

Published in:
Journal européen des droits de l'homme

Publication date:
2017

Document Version
le PDF de l'éditeur

La protection des données à caractère personnel en droit européen

Data Protection in European Law

Jean Herveg & Jean-Marc Van Gyseghem[1]

Résumé

La chronique analyse la contribution de la jurisprudence des juridictions de l'Union européenne et de la Cour européenne des droits de l'homme en matière de la protection des données à caractère personnel pour l'année 2016. La jurisprudence de la Cour européenne des droits de l'homme a concerné la surveillance des individus et de leurs communications, la divulgation d'informations, la protection des données médicales, la filiation, la protection de la réputation, la responsabilité éditoriale des sites web ainsi que le droit d'accès des individus aux données détenues par des autorités publiques. La jurisprudence des juridictions de l'Union européenne a porté sur la délimitation du champ d'application de la protection des données, les mécanismes de légitimation des traitements de données, la conservation des données et le droit d'accès à l'information.

Abstract

The chronicle analyses the contribution of the case-law from European jurisdictions and from the European Court of Humans Rights to data protection. The cases brought before the European Court of Humans Rights concerned the monitoring of individuals and their communications, the disclosure of personal data, the protection of medical data, filiation matters, the protection of one's reputation, the editorial responsibility of websites and the right of access to personal data. The case-law from the European jurisdictions concerned the scope of data protection, the legitimacy mechanisms for data processing, data retention and the right of access to information.

La protection des données est une discipline juridique qui étudie la protection des individus face à l'utilisation d'informations qui les concernent. Cette protection se réalise, d'une part, par l'imposition de règles à respecter lors de l'utilisation d'informations qui les concernent et, d'autre part, par l'attribution à la personne concernée de droits subjectifs à exercer sur les informations qui la concernent. Au niveau européen, c'est le droit au respect de la vie privée qui fonde cette protection sous ces deux aspects. C'est ce droit qui justifie que les individus soient en droit de s'attendre à ce que des règlementations encadrent l'utilisation d'informa-

[1] This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements n° 688520 (TeSLA) & 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant 16.0136 730953. La publication ne reflète que l'opinion de ses auteurs et n'engage en rien la Commission européenne ni le SERI.

tions qui les concernent (ils ont un droit à la protection des données comme le proclame à juste titre l'article 8 de la Charte des droits fondamentaux de l'Union européenne), et c'est toujours lui qui justifie que ces mêmes individus disposent de droits à faire valoir sur les informations qui les concernent. Les travaux du Conseil de l'Europe en matière de protection des données se sont immédiatement prévalus du droit au respect de la vie privée, ce qui se traduira par l'adoption de la Convention (n° 108) pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel et de multiples recommandations sectorielles ou thématiques en matière de protection des données. Dans le même temps, la jurisprudence de la Cour européenne des droits de l'homme contribue à la protection des données dans le cadre du contentieux dont elle est saisie sur pied de l'article 8 de la Convention européenne des droits de l'homme. Comme en toute matière, le rôle de la Cour européenne des droits de l'homme ne se réduit pas, bien évidemment, à assurer une protection minimaliste mais bien à garantir une protection concrète (réelle) et effective des droits des individus et, en particulier, ici, en matière de protection des données. Durant la période couverte, cette protection a été assurée tant en matière de surveillance des individus et de leurs communications, qu'en matière de divulgation d'informations, de protection des données médicales, de filiation, de protection de la réputation, de responsabilité éditoriale des sites web d'information et de droit d'accès aux informations détenues par des autorités publiques[2]. Au niveau de l'Union européenne, la protection des données est, encore à ce jour, assurée par la directive 95/46/CE 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, qui sera remplacée par le règlement général sur la protection des données (dénommé ci-après RGDP) à partir du 25 mai 2018. La jurisprudence actuelle de la Cour de justice de l'Union européenne en matière de protection des données conserve donc toute sa pertinence en raison de la filiation et de la continuité vantées entre ces deux derniers instruments juridiques.

I. La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme

A. La protection contre les mesures de surveillance

1. *L'appréciation de la qualité de victime d'une mesure de surveillance secrète*

Les individus ne peuvent pas toujours établir le fait qu'ils ont concrètement fait l'objet d'une mesure de surveillance secrète. Les États poursuivis leur reprochent, en conséquence, de ne pas prouver leur qualité de « victime », espérant ainsi

[2] À propos de la saisie et de la copie de clés USB et d'un disque dur externe lors de perquisitions, et de la protection du secret professionnel d'avocat, voy. l'arrêt du 20 décembre 2016 (*Lindstrand Partners Advokatbyra AB c. Suède*, n° 18700/09).

obtenir que la Cour déclare la requête irrecevable. Toutefois, conformément à sa jurisprudence, afin de savoir si un individu peut se prévaloir de la qualité de victime d'une ingérence dans le droit au respect de sa vie privée par la seule existence d'une législation autorisant la surveillance secrète (donc même lorsqu'il ne peut pas établir qu'il a été concrètement l'objet d'une mesure de surveillance), la Cour prend en considération les éléments suivants[3] :

1° la portée de la législation autorisant les mesures de surveillance secrète en examinant si le requérant est susceptible d'être concerné soit parce qu'il appartient à un groupe de personnes visé par la législation ou parce que la législation affecte directement toutes les utilisations de services de communications par la mise en place d'un système dans lequel tout le monde peut voir ses communications être interceptées ;

2° l'existence de recours au niveau national tout en tenant compte de leur effectivité.

2. *L'ingérence dans l'exercice du droit au respect de la vie privée*

a. L'interception des communications téléphoniques et hertziennes

Les communications téléphoniques et hertziennes se trouvent comprises dans les notions de « vie privée » et de « correspondance ». En conséquence, leur interception, la mémorisation des données ainsi obtenues et leur éventuelle utilisation dans le cadre des poursuites pénales s'analysent en une « ingérence d'une autorité publique » dans la jouissance d'un droit garanti par l'article 8.1 de la Convention[4]. De la même façon, le contrôle des communications électroniques et des transmissions de données informatiques, ainsi que l'enregistrement des données collectées de cette façon, constituent autant d'ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée des requérants[5].

S'agissant de la poursuite d'un but légitime et de la nécessité de la mesure dans une société démocratique, la Cour a répété que les pouvoirs de surveillance secrète des citoyens ne sont acceptables que dans la mesure où ils sont strictement nécessaires pour la protection des institutions démocratiques[6].

[3] Cour eur. D.H., arrêt du 12 janvier 2016, *Szabo & Vissy c. Hongrie*, n° 37138/14, § 36.
[4] Cour eur. D.H., décision du 23 février 2016, *Capriotti c. Italie*, n° 28819/12, § 43 ; arrêt du 25 octobre 2016, *Basic c. Croatie*, n° 22251/13, § 32.
[5] Cour eur. D.H., arrêt du 12 janvier 2016, *Szabo & Vissy c. Hongrie*, n° 37138/14, §§ 52-53.
[6] *Ibid.*, §§ 54-55.

b. La surveillance secrète d'un assuré par une compagnie d'assurances

À propos de la surveillance secrète d'un assuré par une compagnie d'assurances (revêtant en l'espèce la qualité d'autorité publique), la Cour a réitéré sa position qui consiste à considérer que la surveillance des activités d'un individu en utilisant un équipement vidéo ou photographique, dans la mesure où il s'agit d'un usage normal des caméras de sécurité en tant que telles, que ce soit dans la rue ou dans des endroits publics, et que cela poursuive un but légitime et prévisible, ne pose pas de problème au regard de l'article 8. Toutefois, des questions de vie privée peuvent se poser à propos de l'enregistrement des données et du caractère systématique ou permanent de cet enregistrement[7]. À cet égard, la Cour prend en considération la question de savoir s'il y a eu un regroupement d'informations à propos d'un individu en particulier, s'il y a eu traitement ou utilisation de données à caractère personnel ou s'il y a eu une publication du matériel concerné dans une mesure ou un degré qui excède ce qui est normalement prévisible[8].

3. *Les exigences minimales auxquelles doit répondre la loi qui autorise les mesures de surveillance secrète*

Pour éviter les abus de pouvoirs en matière de surveillance secrète, la loi doit répondre aux mesures minimales de protection suivantes[9] :

1° déterminer la nature des infractions qui peuvent donner lieu à la mesure de surveillance ;

2° définir les catégories de personnes susceptibles d'avoir leur téléphone être mis sous écoute ;

3° limiter la durée de la surveillance téléphonique ;

4° prévoir la procédure à suivre pour examiner, utiliser et conserver les données collectées ;

5° prévoir les précautions à prendre quand les données collectées sont communiquées à d'autres parties ;

6° fixer les circonstances dans lesquelles les enregistrements peuvent ou doivent être effacées ou détruites.

[7] Cour eur. D.H., arrêt du 18 octobre 2016, *Vukota-Bojic c. Suisse*, n° 61838/10, § 55.
[8] *Ibid.*, § 56.
[9] *Ibid.* Voy. aussi en ce sens : l'arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, § 69.

4. *L'exigence de garanties appropriées et effectives contre les abus en matière de surveillance secrète*

Si l'État dispose d'une marge d'appréciation dans le choix des mesures à mettre en œuvre pour protéger la sécurité nationale lorsqu'il met en balance la protection de la sécurité nationale par des mesures de surveillance secrète au regard de l'importance de l'ingérence dans l'exercice du droit au respect de la vie privée des individus[10], vu le risque qu'un tel système de surveillance puisse nuire ou détruire la démocratie sous le couvert de sa défense, la Cour doit toutefois être convaincue de la présence de garanties appropriées et effectives contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre[11]. Cette évaluation dépend de toutes les circonstances de la cause comme :

1° la nature, la portée et la durée des mesures qui sont possibles ;

2° les raisons requises pour les ordonner ;

3° les autorités compétentes pour les autoriser, les mettre en œuvre et les contrôler ;

4° ainsi que le type de recours fournis par le droit interne.

De cette façon, la Cour peut déterminer si les procédures pour contrôler la décision et la mise en œuvre de ces mesures permettent de les maintenir dans les limites de ce qui est nécessaire dans une société démocratique[12].

L'examen et le contrôle des mesures de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle ait cessé. *Concernant les deux premières phases*, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. Puisqu'on empêche forcément l'intéressé d'introduire un recours effectif ou de prendre une part directe à un contrôle quelconque, il est indispensable que les procédures existantes procurent en elles-mêmes des garanties appropriées et équivalentes pour sauvegarder les droits de l'individu. Il faut de surcroît, pour ne pas dépasser les bornes de la nécessité, respecter aussi fidèlement que possible, dans les procédures de contrôle, les valeurs d'une société démocratique. En un

[10] Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent (Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, § 101 et la décision du 23 février 2016, *Capriotti c. Italie*, n° 28819/12, § 54).

[11] Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, § 101. Voy. aussi la décision du 23 février 2016, *Capriotti c. Italie*, n° 28819/12, § 54.

[12] Cour eur. D.H., décision du 23 février 2016, *Capriotti c. Italie*, n° 28819/12, § 57. Voy. aussi en ce sens : Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, §§ 70 et 101. Les mêmes exigences s'appliquent à la surveillance secrète d'un assuré par une compagnie d'assurances revêtant la qualité d'autorité publique (en ce sens, voy. l'arrêt du 18 octobre 2016, *Vukota-Bojic c. Suisse*, n° 61838/10, § 68).

domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le pouvoir judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière.

Quant au troisième stade, c'est-à-dire lorsque la surveillance a cessé, la question de la notification *a posteriori* de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci ou si, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure. Toutefois, il peut ne pas être possible en pratique d'exiger une notification *a posteriori* de la mesure de surveillance dans tous les cas. L'activité ou le danger qu'un ensemble de mesures de surveillance vise à combattre peut subsister pendant des années, voire des décennies, après la levée de ces mesures. Une notification *a posteriori* à chaque individu touché par une mesure désormais levée risquerait de compromettre le but à long terme qui motivait à l'origine la surveillance. En outre, pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignement, leurs champs d'activité et même, le cas échéant, l'identité de leurs agents. Dès lors, l'absence de notification ultérieure aux personnes touchées par des mesures de surveillance secrète, dès la levée de celles-ci, ne saurait en soi justifier la conclusion que l'ingérence n'était pas « nécessaire, dans une société démocratique », car c'est précisément cette absence d'information qui assure l'efficacité de la mesure constitutive de l'ingérence. Cependant, il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la mesure[13].

5. *L'autorisation et le contrôle des mesures de surveillance secrète*

L'exigence d'une autorisation judiciaire préalable de la mesure de surveillance est de nature à limiter le pouvoir discrétionnaire des autorités notamment grâce à une pratique ou une interprétation judiciairement établie qui permette de vérifier s'il existe des raisons suffisantes pour intercepter les communications d'une personne en particulier dans chaque cas. Ce n'est que dans cette mesure que les mesures urgentes ne seront utilisées qu'à bon escient et uniquement dans les cas qui le requièrent[14].

[13] Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, § 73 ; Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, §§ 33, 34 et 86.
[14] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, § 73.

S'il peut être débattu de savoir qui du juge ou d'un ministre du gouvernement est le mieux placé pour autoriser ou contrôler des mesures de surveillance secrète, la Cour considère, par contre, qu'il n'en va pas de même quant à savoir qui doit analyser les buts et les moyens de la mesure en termes de stricte nécessité dans une société démocratique[15]. À cet égard, s'il peut être accepté qu'une autorité non judiciaire puisse autoriser une mesure de surveillance secrète si elle est suffisamment indépendante du gouvernement, il n'en demeure pas moins que la nature politique de l'autorisation et du contrôle augmente le risque d'abus. La Cour rappelle, à cet égard, que la primauté du droit implique que l'ingérence d'une autorité publique dans les droits d'un individu soit soumise à un contrôle effectif qui, en principe, doit revenir au pouvoir judiciaire (en tout cas, en dernier ressort), ce dernier devant offrir les meilleures garanties d'indépendance, d'impartialité, ainsi que l'existence d'une procédure adéquate. En règle, c'est donc normalement à un juge avec une certaine expertise que doit revenir le contrôle des mesures de surveillance secrète et toute exception à ce principe doit faire l'objet d'un contrôle minutieux. Une autorisation préalable n'est pas une exigence absolue s'il existe un contrôle judiciaire extensif *a posteriori* qui permet de contrebalancer l'absence d'autorisation judiciaire préalable. Toutefois, dans certains cas, comme lors de la surveillance secrète de médias, une autorisation judiciaire préalable est nécessaire[16].

Même si dans certaines circonstances, l'autorisation d'interception de communications téléphoniques par une autorité non judiciaire peut être compatible avec la Convention, le contrôle judiciaire représente une protection importante contre l'arbitraire à toutes les étapes de la surveillance secrète, pourvu que le contrôle soit effectif dans la pratique aussi bien qu'en droit. L'effectivité du contrôle signifie que l'autorité de contrôle doit être en mesure de vérifier si les mesures litigieuses sont ordonnées et exécutées de manière légale. S'agissant d'un contrôle *a posteriori*, le requérant doit, à tout le moins, recevoir une information suffisante en ce qui concerne l'existence d'une autorisation et un minimum d'informations sur la décision qui a autorisé la surveillance secrète[17].

L'autorisation judiciaire qui ne contient aucun raisonnement qui permet de justifier le recours à la mesure de surveillance secrète, combinée avec la pratique des juridictions nationales consistant à contourner cette nécessité par une justification *a posteriori* du recours à la surveillance secrète, en contradiction avec le droit national, ne garantit donc pas en pratique les mesures de protection adéquates contre les divers abus possibles. En conséquence, ces pratiques ne sont pas compatibles avec l'exigence d'être prévues par la loi et elles ne sont pas suffisantes pour contenir cette ingérence à ce qui est nécessaire dans une société démocratique[18].

[15] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, nº 19602/06, § 76.
[16] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, nº 19602/06, § 77.
[17] Cour eur. D.H., arrêt du 31 mars 2016, *Santare et Labaznikovs c. Lettonie*, nº 34148/07, §§ 54-55.
[18] Cour eur. D.H., arrêt du 25 octobre 2016, *Basic c. Croatie*, nº 22251/13, § 34.

Dans le cas de la surveillance secrète d'un assuré par la compagnie d'assurances, la Cour a relevé les éléments suivants[19] :

1° l'absence de toute description des procédures à suivre pour autoriser ou contrôler la mise en œuvre de mesures de surveillance secrète dans le contexte particulier des litiges d'assurance ;

2° l'absence de toute précision à propos de la durée maximale des mesures de surveillance ou la possibilité de les contester en justice, ce qui conférait aux compagnies d'assurances un large pouvoir discrétionnaire pour décider des circonstances qui justifient une telle surveillance et sa durée ;

3° l'absence de toute disposition sur les procédures à suivre pour conserver, accéder, examiner, utiliser, communiquer ou détruire les données collectées par les mesures secrètes de surveillance. Il n'était donc pas clair de savoir où et combien de temps le rapport qui contient les prises d'images et de photographies pouvait être conservé, qui pouvait y avoir accès et si la personne concernée disposait des moyens légaux de contester ce qui était fait de ce rapport, ce qui induit nécessairement le risque d'accès non autorisé ou la divulgation non autorisée des matériaux de surveillance.

En conséquence, et nonobstant le fait que cette surveillance est jugée moins intrusive que l'interception des communications téléphoniques, le droit national n'indiquait pas, en l'espèce, avec suffisamment de clarté l'étendue et les modalités d'exercice du pouvoir discrétionnaire conféré aux compagnies d'assurances agissant en qualité d'autorités publiques dans les litiges d'assurance pour réaliser la surveillance secrète des personnes assurées. C'est, en particulier, les mesures de protection contre l'abus qui manquaient[20].

En tout cas, l'absence de garanties adéquates et effectives contre les abus éventuels des pouvoirs de surveillance de l'État quant aux écoutes autorisées par un tribunal dans le cadre d'une information judiciaire a pour conséquence que la mesure de surveillance n'est pas « prévue par la loi »[21].

6. *Les contraintes liées à l'exigence de prévisibilité de la loi qui autorise les mesures de surveillance secrète – La qualité de la loi*

L'ingérence doit être prévue par la loi et la qualité de la loi, à cet égard, implique non seulement l'accessibilité et la prévisibilité de la loi nationale, mais aussi que les mesures de surveillance secrète ne soient mises en œuvre que lorsque c'est

[19] Cour eur. D.H., arrêt du 18 octobre 2016, *Vukota-Bojic c. Suisse*, n° 61838/10, §§ 74-77.
[20] *Ibid.*, § 77.
[21] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, §§ 36-37.

nécessaire dans une société démocratique en fournissant les protections et garanties appropriées et effectives contre les abus[22].

En matière de surveillance secrète, la prévisibilité dans la mise en œuvre de la loi n'implique pas que les individus soient informés que les autorités sont susceptibles d'intercepter ses communications de manière à lui permettre d'adapter son comportement en conséquence. En conséquence, spécialement lorsqu'un tel pouvoir reconnu au gouvernement s'exerce en secret, le risque d'arbitraire est évident. Il est donc essentiel d'avoir des règles claires et détaillées sur l'interception des communications téléphoniques, notamment quand la technologie devient de plus en plus sophistiquée. Le droit national doit donner aux citoyens des indications claires sur les circonstances et les conditions dans lesquelles les autorités publiques sont autorisées à recourir à de pareilles mesures de surveillance[23].

La Cour reconnaît à cet égard le besoin d'éviter une rigidité excessive dans la formulation des dispositions légales en la matière ainsi que le besoin de tenir compte du changement des circonstances et qu'en conséquence, beaucoup de lois sont inévitablement écrites dans des termes plus ou moins vagues, dans une certaine mesure. Il n'est donc pas requis que la loi liste de manière détaillée toutes les situations dans lesquelles le gouvernement peut décider d'une mesure de surveillance secrète. La simple référence à des menaces terroristes ou à des opérations d'intervention est en principe suffisante pour informer adéquatement les citoyens[24].

Mais il serait contraire à la primauté du droit qu'un pouvoir discrétionnaire reconnu au gouvernement en matière de sécurité nationale puisse être formulé sans limite, d'autant plus que l'application des mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public. En conséquence, la Cour exige que la loi indique l'étendue du pouvoir ainsi conféré aux autorités compétentes et la manière d'exercer ce pouvoir discrétionnaire avec suffisamment de clarté, en tenant compte du but légitime de la mesure de surveillance, de façon à donner aux individus une protection adéquate contre les ingérences arbitraires[25].

---

[22] *Ibid.*, § 59.
[23] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, § 62. Voy., en ce sens, également : Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, § 67 ; arrêt du 21 juin 2016, *Oleynik c. Russie*, n° 23559/07§ 74 ; arrêt du 8 novembre 2016, *Figueiredo Teixeira c. Andorre*, n° 72384/14, § 40 ; arrêt du 31 mars 2016, *Santare et Labaznikovs c. Lettonie*, n° 34148/07, § 53. Dans le même sens à propos de la surveillance secrète d'un assuré par la compagnie d'assurances : Cour eur. D.H., arrêt du 18 octobre 2016, *Vukota-Bojic c. Suisse*, n° 61838/10, § 67. Pour un cas d'utilisation d'une caméra de surveillance dans une cellule de prison en contradiction avec le droit national, voy. l'arrêt du 6 décembre 2016, *Vasilica Mocanu c. Roumanie*, n° 43545/13.
[24] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, § 64.
[25] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, § 65. Voy. aussi en ce sens : Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, § 68 ; arrêt du 21 juin 2016, *Oleynik c. Russie*, n° 23559/07, § 74.

Au vu des développements technologiques considérables qui permettent une surveillance de masse tant en ce qui concerne la quantité d'individus concernés que la quantité d'informations collectées, de l'exigence de la nécessité de la mesure dans une société démocratique et de l'existence de mesures de protection appropriées et effectives contre les abus, la Cour considère que la mesure de surveillance secrète n'est acceptable que si elle est strictement nécessaire, en général, pour la protection des institutions démocratiques et, de plus, si elle est strictement nécessaire, en particulier, pour obtenir une information vitale dans une opération individuelle. À défaut, la mesure de surveillance ouvrirait la voie à des abus par des autorités disposant de technologies formidables[26].

La Cour a rappelé qu'en l'absence de règles spécifiques et détaillées, lorsqu'un pouvoir discrétionnaire conféré par la loi aux autorités pour ordonner l'interception de conversations au moyen d'un appareil de radio transmission n'est subordonné à aucune condition, que la portée et les modalités d'exercice de ce pouvoir ne sont pas définies et qu'aucune autre garantie spécifique n'est prévue, le recours à cette technique de surveillance n'est pas entouré des garanties adéquates contre les divers abus possibles dès lors que sa mise en œuvre est susceptible d'arbitraire et est incompatible avec la condition de légalité[27].

La Cour a eu l'occasion de revenir sur la technique du « comptage » comme moyen d'obtention de données (c'est un mécanisme qui enregistre les numéros formés sur un appareil de téléphone donné ainsi que l'heure et la durée de chaque appel). À cet égard, elle a admis que l'exploitation des éléments ainsi collectés pouvait être problématique sous l'angle de l'article 8. Il faut examiner, notamment, l'organe qui a autorisé la transmission de données à l'insu du requérant. La précision requise de la législation interne (qui ne peut prévoir toutes les hypothèses) dépend dans une large mesure du contenu de l'instrument en question, du domaine qu'il est censé couvrir ainsi que du nombre et de la qualité de ceux à qui il s'adresse. La pratique qui consiste à transmettre les données obtenues au moyen d'un système de « comptage » ne soulève pas, en tant que telle, de problème. Par contre, c'est la transmission de ces données directement à la demande d'un service de police, d'une autorité administrative ou d'un ministre, qui pose problème. La Cour a jugé que la procédure andorrane offrait de nombreuses garanties contre les comportements arbitraires[28] :

1° c'est toujours un juge (Batlle) qui autorise, en amont, la mesure ;

2° la durée maximale de la mesure est fixée par la loi et intéresse seulement les délits les plus graves ;

---

[26] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, § 73.
[27] Cour eur. D.H., arrêt du 21 juin 2016, *Oleynik c. Russie*, n° 23559/07, § 75. Dans cet arrêt, la Cour a souligné l'absence de décision judiciaire autorisant les écoutes ainsi que l'absence de garanties adéquates contre les divers abus possibles. L'ingérence a donc été considérée comme n'étant pas prévue par la loi. Cet arrêt se réfère principalement à l'arrêt *Bykov c. Russie* du 10 mars 2009 prononcé en Grande Chambre (n° 4378/02, §§ 78-79).
[28] Cour eur. D.H., arrêt du 8 novembre 2016, *Figueiredo Teixeira c. Andorre*, n° 72384/14, §§ 40, 41 et 43.

3° le requérant peut toujours contester la légalité de la preuve obtenue au cours du procès.

7. *La nécessité de renforcer le contrôle des mesures de surveillance secrète en cas de partage d'informations entre gouvernements*

S'il n'y a pas lieu de mettre en cause le partage entre les gouvernements d'informations provenant de mesures de surveillance secrète, il s'agit toutefois d'un facteur à prendre en compte en ce qui concerne le contrôle extérieur et les recours. C'est, en effet, dans ce contexte que le contrôle externe *a posteriori*, de préférence judiciaire, des activités de surveillance secrète, prend toute son importance en renforçant la conviction des citoyens que les garanties de l'État de droit sont respectées même dans ce secteur délicat et que les recours sont mis à disposition en cas d'abus avéré. L'importance de ce contrôle ne peut pas être mésestimée au vue de l'ampleur des données collectées par les autorités en utilisant des méthodes extrêmement efficaces et traitant des quantités énormes de données, potentiellement relatives à tout individu qui serait connecté d'une manière ou de l'autre à des projets d'attaque terroriste[29].

8. *La reconnaissance de la nécessité d'une loi conférant des pouvoirs de surveillance secrète en cas de terrorisme*

La Cour reconnait que l'exigence d'une autorisation judiciaire préalable n'est pas toujours possible notamment au vu de la nature du terrorisme actuel. Elle peut donc accepter, comme elle l'a déjà fait dans le passé, que l'existence d'une législation conférant des pouvoirs de surveillance secrète sur la correspondance et les télécommunications soit, dans des circonstances exceptionnelles, nécessaire dans une société démocratique dans l'intérêt de la sécurité nationale ou de la prévention des crimes et délits[30].

La Cour rappelle toutefois que la Convention impose une certaine forme de conciliation entre les impératifs de la défense de la société démocratique et ceux de la sauvegarde des droits individuels. Dans le contexte de l'article 8, cela signifie qu'il faut rechercher un équilibre entre l'exercice par l'individu du droit au respect de la vie privée et la nécessité d'imposer une surveillance secrète pour protéger la société démocratique dans son ensemble. Quant à la décision de placer une personne sous surveillance, elle rappelle que l'existence de soupçons plausibles présuppose celle de faits ou de renseignements propres à persuader un observateur objectif que l'individu en cause peut avoir commis l'infraction en question. Les faits donnant naissance à des soupçons ne doivent pas être du même niveau

[29] Cour eur. D.H., arrêt du 7 juin 2016, *Cevat Özel c. Turquie*, n° 19602/06, § 79.
[30] *Ibid.*, § 80.

que ceux qui sont nécessaires pour justifier une condamnation ou même pour porter une accusation, ce qui intervient dans la phase suivante de la procédure de l'enquête pénale[31].

9. *La surveillance des communications électroniques dans le cadre des relations de travail*

Conformément à sa jurisprudence, la Cour a répété que les courriers électroniques envoyés depuis le travail étaient protégés par l'article 8 de la Convention de la même manière que les conversations téléphoniques depuis le lieu du travail.

En l'absence d'information sur la surveillance des communications, la personne concernée se voit reconnaître une attente raisonnable en ce qui concerne le caractère privé des appels réalisés depuis un téléphone professionnel. La même attente existe en ce qui concerne le courrier électronique et l'usage de l'Internet dans le cadre du travail. De la même façon, un individu a une attente raisonnable au respect du caractère privé de ses effets personnels dans le lieu de son travail[32].

La situation est toutefois différente lorsque l'employeur a formellement interdit d'utiliser les ordinateurs et les ressources de l'entreprise à des fins privées. Mais, même dans ce cas, la vie privée du travailleur est concernée par le fait que son employeur a surveillé sa messagerie professionnelle Yahoo, notamment en accédant au contenu des messages et en utilisant leur retranscription devant les juridictions du travail contre le travailleur, d'autant que certains messages étaient d'ordre strictement privé. Néanmoins, la Cour a considéré qu'il n'était pas déraisonnable, dans ce cas, pour l'employeur de vouloir vérifier que ses employés réalisaient bien leurs tâches professionnelles durant les heures de travail, surtout lorsque l'employé a affirmé ne pas avoir utilisé la messagerie à des fins privées, que le contrôle a été limité dans son étendue et proportionné, et que l'usage des données dans le cadre du litige devant les juridictions du travail s'est limité à ce qui était nécessaire[33].

10. *La surveillance du courrier et des conversations téléphoniques dans un centre d'éducation fermé pour mineurs d'âge*

Le pouvoir discrétionnaire de contrôler la correspondance des mineurs, c'est-à-dire sans distinction entre les catégories de destinataires (et notamment l'absence de régime spécial pour la correspondance avec les avocats ou les organisations non gouvernementales de protection des droits de l'enfant), sans limite quant à la durée de la mesure et sans indication quant aux raisons qui pourraient la justifier

[31] Cour eur. D.H., arrêt du 7 juin 2016, *Karabeyoglu c. Turquie*, n° 30083/10, §§ 102-103.
[32] Cour eur. D.H., arrêt du 12 janvier 2016, *Barbulescu c. Roumanie*, n° 61496/08, §§ 36-37.
[33] Cour eur. D.H., arrêt du 12 janvier 2016, *Barbulescu c. Roumanie*, n° 61496/08, §§ 44-45 et 59-60.

pas plus que sur les conditions de son contrôle, n'est pas conforme à l'article 8 de la Convention. La Cour condamne ainsi le contrôle automatique et indifférencié de toute la correspondance que le mineur d'âge en centre fermé pourrait entretenir avec le monde extérieur.

Ensuite, la Cour a rappelé que les communications téléphoniques qui se déroulaient sous la surveillance des membres du personnel du centre fermé, étaient privées de toute confidentialité. Pour parvenir à justifier l'application d'un régime indifférencié d'autorisation et de contrôle des communications téléphoniques, sans tenir compte de toute appréciation individuelle des exigences en termes de sécurité que pouvait requérir la personnalité de chacun des mineurs, alors qu'il est essentiel de permettre aux enfants ainsi placés de maintenir un contact réel avec leur famille proche, il aurait fallu que le Gouvernement analyse scrupuleusement les risques auxquels cette mesure était censée répondre (ce qu'il n'a pas fait). En conclusion, un régime de contrôle automatique de la correspondance, opéré sans aucune distinction quant au type d'échanges, et la surveillance des communications téléphoniques, excluant toute confidentialité de celles-ci, auxquels la requérante a été soumise dans le centre d'éducation fermé, ne rencontrent pas l'exigence de la nécessité dans une société démocratique[34].

B. La protection contre les enregistrements vidéo

L'enregistrement vidéo d'une arrestation sans le consentement de la personne concernée constitue une ingérence dans son droit à l'image qui fait partie intégrante de la notion de vie privée[35].

La diffusion de l'enregistrement vidéo d'une perquisition au cours de laquelle les personnes sont montrées dans des postures humiliantes et qu'aucune précaution minimale n'a été prise pour protéger leur vie privée (masquer les corps et les visages, les images ayant été prises dans des espaces privés), alors qu'il existe des procédés moins attentatoires à la vie privée des requérants qui pouvaient légitimement s'attendre à une protection accrue de leur vie privée en leur qualité de « personnes ordinaires » et qui auraient permis d'informer de manière tout aussi satisfaisante le public sur les investigations en cours, est une atteinte injustifiée dans le droit à la protection de la vie privée des personnes concernées[36].

[34] Cour eur. D.H., arrêt du 19 mai 2016, *D.L. c. Bulgarie*, n° 7472/14, §§ 106, 110 et 115.
[35] Cour eur. D.H., arrêt du 9 juin 2016, *Popovi c. Bulgarie*, n° 39651/11, § 98.
[36] Cour eur. D.H., arrêt du 26 avril 2016, *Amarandei et autres c. Roumanie*, n° 1443/10, §§ 235-236.

C. La protection contre les divulgations d'informations

1. *La divulgation d'informations judiciaires*

La fuite d'informations judiciaires confidentielles dans la presse constitue une ingérence injustifiée dans la vie privée des personnes concernées[37].

2. *La divulgation d'informations enregistrées au cours d'une audience*

a. Le rappel des principes relatifs à la liberté d'expression et à la presse

La liberté d'expression constitue l'un des fondements essentiels d'une société démocratique et les garanties à accorder à la presse revêtent donc une importance particulière.

La presse joue un rôle éminent dans une société démocratique : si elle ne doit pas franchir certaines limites, tenant notamment à la protection de la réputation et aux droits d'autrui ainsi qu'à la nécessité d'empêcher la divulgation d'informations confidentielles, il lui incombe néanmoins de communiquer, dans le respect de ses devoirs et de ses responsabilités, des informations et des idées sur toutes les questions d'intérêt général. En particulier, on ne saurait penser que les questions dont connaissent les tribunaux ne puissent, auparavant ou en même temps, donner lieu à discussion ailleurs, que ce soit dans des revues spécialisées, la grande presse ou le public en général. À la fonction des médias consistant à communiquer de telles informations et idées s'ajoute le droit, pour le public, d'en recevoir. Toutefois, il convient de tenir compte du droit de chacun de bénéficier d'un procès équitable qui comprend le droit à un tribunal impartial. Comme la Cour l'a déjà souligné, « les journalistes qui rédigent des articles sur des procédures pénales en cours doivent s'en souvenir, car les limites du commentaire admissible peuvent ne pas englober des déclarations qui risqueraient, intentionnellement ou non, de réduire les chances d'une personne de bénéficier d'un procès équitable ou de saper la confiance du public dans le rôle tenu par les tribunaux dans l'administration de la justice pénale ».

Les États contractants disposent d'une certaine marge d'appréciation pour juger de la nécessité et de l'ampleur d'une ingérence dans la liberté d'expression. Mais il

[37] *Ibid.*, § 220. Dans cet arrêt, la Cour a précisé que la perquisition et la saisie d'objets personnels portaient atteinte aux droits garantis par l'article 8 lorsqu'elles présentent un caractère massif et indifférencié et en l'absence de contrôle *a posteriori* effectif (§ 228). À propos de la communication de l'enregistrement vidéo par la police de l'arrestation du requérant aux chaînes de télévision : voy. l'arrêt du 31 mars 2016 (*Alexey Petrov c. Bulgarie*, n° 30336/10). À propos de l'achat par les services secrets allemands de données relatives à des fraudes fiscales, voy. l'arrêt du 6 octobre 2016, *K.S.et M.S. c. Allemagne*, n° 33696/11.

n'y a guère de place pour des restrictions à la liberté d'expression dans le domaine des questions d'intérêt général[38].

b. Les critères à prendre en compte

Lors de la divulgation d'informations enregistrées au cours d'une audience, la liberté d'expression se heurte au droit des témoins au respect de leur vie privée ainsi qu'à l'autorité et à l'impartialité de l'appareil judiciaire[39], qu'il faut mettre en balance. À cet égard, la Cour retient les critères suivants :

1° la contribution du reportage à un débat d'intérêt général ;

2° le comportement de la personne ;

3° le contrôle exercé par les juridictions internes ;

4° la proportionnalité de la sanction.

D. Les listes de collaborateurs dans les anciens pays de l'Est (le phénomène de la lustration)

La Cour a répété que les mesures de lustration poursuivaient un but légitime et qu'en conséquence, la conservation des dossiers des services de sécurité du régime antérieur n'était pas en soi contraire à la Convention. La décision de maintenir le nom d'un individu dans les listes des collaborateurs de l'ancien régime a un profond effet sur la vie privée. Il faut tenir compte de l'obligation qui était faite aux individus de collaborer avec les services de sécurité du régime antérieur dans la mise en balance des intérêts de la sécurité nationale et de la protection de la personne concernée. En l'espèce, la Cour a considéré que la mesure litigieuse n'était pas nécessaire (proportionnée) dans une société démocratique surtout au vu des conséquences pour la vie privée de la personne concernée. Elle a souligné le fait qu'il fallait aussi tenir compte de l'écoulement du temps que ce soit à propos de la mise en place d'un système démocratique ou de la date de la collaboration[40].

E. La protection des données médicales

La conservation et le partage de données relatives à la vie privée d'un individu et, plus spécialement, de données médicales personnelles, constituent des ingérences au sens de l'article 8 de la Convention. L'enregistrement d'informations relatives à des aliénés ne sert pas que l'intérêt légitime d'assurer le bon fonctionnement

[38] Cour eur. D.H., arrêt du 22 mars 2016, *Pinto Coelho c. Portugal (n° 2)*, n° 48718/11, §§ 36-40.
[39] Cour eur. D.H., arrêt du 22 mars 2016, *Pinto Coelho c. Portugal (n° 2)*, n° 48718/11, § 41.
[40] Cour eur. D.H., arrêt du 21 janvier 2016, *Ivanovski c. l'ancienne République yougoslave de Macédoine*, n° 29908/11, §§ 167, 179, 177, 182, 185 et 186.

d'un service public hospitalier; il sert aussi à protéger les droits des patients eux-mêmes. L'inscription du nom de la requérante sur le registre de l'hôpital des personnes souffrant de troubles psychiatriques et les communications internes à l'hôpital nécessaires au fonctionnement des institutions de santé et les communications externes avec les tribunaux saisis par la requérante en contestation de son diagnostic étaient nécessaires pour le bon fonctionnement des hôpitaux et la prise de décisions par les juridictions. Rien ne permet de considérer que les informations ont été divulguées au public ou utilisées à d'autres fins que de choisir les soins de santé les plus adaptés pour la requérante[41].

1. *La nécessité de protéger les données relatives à la santé*

Les informations personnelles relatives à un patient relèvent de sa vie privée. La protection des données à caractère personnel, dont les données médicales ne sont pas les moindres, est d'une importance fondamentale pour la jouissance du droit au respect de la vie privée et familiale. Le respect de la confidentialité des données relatives à la santé est un principe vital dans les systèmes juridiques de tous les États parties à la Convention. Il est crucial non seulement pour préserver le sentiment de vie privée du patient mais aussi pour préserver sa confiance dans la profession médicale et dans les services de santé en général. Sans cette protection, ceux qui ont besoin d'une aide médicale pourraient être dissuadés de révéler de telles informations de nature personnelle et intime qui pourraient être nécessaires pour recevoir les traitements appropriés et même de rechercher pareille aide médicale, mettant par là en danger leur propre santé et, dans le cas de maladies contagieuses, celle de la société. Le droit national doit, en conséquence, fournir des protections appropriées pour prévenir la communication ou la divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme avec les garanties offertes par l'article 8 de la Convention[42].

2. *La divulgation de données relatives à la santé*

La divulgation de dossiers médicaux contenant des données extrêmement personnelles et sensibles sans le consentement du patient concerné, en ce compris des informations relatives à un avortement, par une clinique à un service d'assurance sociale, et par conséquent à un cercle plus large de fonctionnaires, constituait une ingérence dans le droit au respect de la vie privée du patient. La divulgation de données médicales par des institutions médicales au bureau d'un procureur et à l'employeur d'un patient, ainsi que la collecte de données médicales d'un patient par une institution en charge du contrôle de la qualité des soins de santé ont aussi été considérées comme constituant une ingérence dans le droit au respect de la vie privée. En conséquence, l'accès et l'examen des dossiers d'une mère et de ses

[41] Cour eur. D.H., décision du 31 mai 2016, *Malanicheva c. Russie*, n° 50405/06, §§ 13, 15 et 17. La Cour renvoie à un arrêt du 9 juillet 1991 (n° 14461/88) (et non pas de 1992 comme indiqué erronément dans l'arrêt).
[42] Cour eur. D.H., arrêt du 23 février 2016, *Y.Y. c. Russie*, n° 40378/06, § 38.

enfants par une Commission publique en matière de santé sur requête du ministère de la Santé suite aux plaintes de la grand-mère des enfants, sans le consentement de la mère de ceux-ci, constituent une ingérence dans le droit au respect de la vie privée de la mère des enfants[43].

F. Les litiges en matière de filiation

1. *Vie privée, identité et actions en matière de filiation*

La naissance, et singulièrement les circonstances de celle-ci, relèvent de la vie privée de l'enfant, puis de l'adulte, garantie par l'article 8 de la Convention. 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. Ceci inclut l'obtention des informations nécessaires à la découverte de la vérité concernant un aspect important de son identité personnelle, par exemple l'identité de ses géniteurs.

L'établissement d'une filiation peut avoir des répercussions considérables non seulement sur la vie privée et familiale des proches parents du père présumé, mais aussi sur leur situation patrimoniale, ce qui permet au législateur de réglementer les questions liées à la filiation. L'ingérence litigieuse tendait donc à la protection des « droits et libertés d'autrui ».

Pour dire si l'article 8 de la Convention a ou non été observé, la Cour doit non seulement mesurer les intérêts de l'individu à l'intérêt général de la collectivité prise dans son ensemble, mais encore peser les intérêts privés concurrents en jeu. À cet égard, il y a lieu de noter que l'expression « toute personne » figurant à l'article 8 de la Convention s'applique à l'enfant comme au père présumé. D'un côté, il y a le droit à la connaissance de ses origines qui trouve son fondement dans l'interprétation extensive de la notion de vie privée. Les personnes qui se trouvent dans cette situation ont un intérêt vital, défendu par la Convention, à obtenir les informations qui leur sont indispensables pour découvrir la vérité sur un aspect important de leur identité personnelle et dissiper toute incertitude à cet égard. D'un autre côté, on ne saurait nier l'intérêt d'un père présumé à être à l'abri de plaintes tardives se rapportant à des faits qui remontent à de nombreuses années. Enfin, outre les intérêts concurrents qui viennent d'être évoqués peuvent entrer en jeu d'autres intérêts, par exemple ceux de tiers, pour l'essentiel la famille du père présumé, et l'intérêt général avec la sécurité juridique[44].

De même, la reconnaissance et l'annulation d'un lien de filiation touchent directement à l'identité de l'homme ou de la femme dont la parenté est en question.

---

[43] *Ibid.*, §§ 39-40.
[44] Cour eur. D.H., 19 juillet 2016, *Calin et autres c. Roumanie*, n^os^ 25057/11, 34739/11 et 20316/12, §§ 83, 90 et 92. À propos du refus de transcrire l'acte de naissance d'un enfant né par GPA, voy. l'arrêt du 21 juillet 2016, *Foulon et Bouvet c. France*, n^os^ 9063/14 et 10410/14.

De plus, en tant que moyen d'identification personnelle et de rattachement à une famille, le nom d'une personne concerne sa vie privée et familiale[45]. Les procédures en reconnaissance ou en contestation de paternité concernent aussi la « vie privée » du père présumé car elles englobent des aspects importants de l'identité de ce dernier. La possibilité ou non d'établir un lien de filiation relève indéniablement de la « vie privée »[46].

En l'absence de consensus sur la question, la décision de savoir si un individu doit être autorisé à contester la paternité légalement établie à l'égard d'un enfant dont il pense être le père biologique tombe dans la marge d'appréciation des États. Celle-ci est importante lorsqu'il s'agit de mettre en balance les droits fondamentaux concurrents de deux individus. Cette marge d'appréciation n'en demeure pas moins soumise au contrôle de la Cour étant entendu que l'intérêt supérieur de l'enfant concerné doit primer[47].

2. *La possibilité pour un père biologique prétendu de contester une reconnaissance de paternité*

L'article 8 de la Convention impose aux États l'obligation de rechercher s'il est dans l'intérêt de l'enfant de permettre au père biologique de nouer une relation avec le mineur, par exemple en lui accordant un droit de visite. Le père biologique ne devrait pas être complètement empêché d'établir sa paternité ou exclu de la vie de l'enfant sauf s'il y a des raisons impératives liées à l'intérêt supérieur de ce dernier. Cela n'implique pas nécessairement une obligation d'autoriser un père biologique présumé à contester le statut du père légitime. Toutefois, une impossibilité absolue pour un homme prétendant être le père biologique de chercher à établir sa paternité, au seul motif qu'un autre homme a déjà reconnu l'enfant, a été considérée comme méconnaissant l'article 8 de la Convention.

La Cour a rappelé que le fait que les autorités disposaient d'un pouvoir d'appréciation pour décider d'engager ou non une procédure en contestation d'une reconnaissance de paternité n'était pas en soi critiquable. Toutefois, l'absence d'accès direct du père biologique à une procédure lui permettant de faire établir sa paternité, l'absence – en droit interne – de lignes directrices concernant la manière dont le pouvoir discrétionnaire des autorités de contester une reconnaissance de paternité doit être exercé, ainsi que la façon superficielle dont les demandes visant à contester la reconnaissance effectuée par un autre homme ont été examinées, a déjà amené la Cour à conclure à la violation de l'article 8.

La Cour a aussi rappelé que, dans d'autres affaires, elle avait estimé que le refus d'examiner l'action en recherche de paternité du requérant n'avait pas rompu le

[45] Cour eur. D.H., arrêt du 14 janvier 2016, *Mandet c. France*, n° 30955/12, § 44.
[46] Cour eur. D.H., décision du 31 mai 2016, *Gueye c. Italie*, n° 76823/12, § 30. Voy. aussi l'arrêt du 8 décembre 2016, *L.D. et P.K. c. Bulgarie*, n^os^ 7949/11 et 45522/13, § 56.
[47] Cour eur. D.H., arrêt du 14 janvier 2016, *Mandet c. France*, n° 30955/12, §§ 52-53.

juste équilibre et n'avait ainsi pas enfreint l'article 8 dans la mesure où ce refus était fondé non seulement sur le fait que l'enfant avait déjà un lien de filiation établi par reconnaissance ou présomption de paternité, mais aussi sur l'existence d'une relation sociale et familiale entre l'enfant et ses père et mère légitimes ou sur l'appréciation des juridictions internes selon laquelle, dans le cas concret, l'autorisation d'une recherche de paternité n'était pas dans l'intérêt de l'enfant.

Dans toutes ces affaires, la Cour souligne qu'elle avait relevé que l'interdiction pour le père biologique de chercher à établir sa paternité n'était pas absolue et que le droit interne prévoyait des hypothèses où une recherche de paternité était recevable, par exemple lorsque la paternité légitime ne correspondait pas à la réalité sociale et familiale ou encore lorsque le père biologique présumé avait eu pendant la période de la conception une relation durable avec la mère, qui avait interrompu sa cohabitation avec le père légitime. La Cour tenait également compte du fait que le processus décisionnel ayant abouti à l'interdiction en question comportait certaines garanties telles que l'examen circonstancié des faits de la part des autorités compétentes, la mise en balance des différents intérêts en jeu, et notamment de l'intérêt supérieur de l'enfant, ou la possibilité pour le requérant d'exposer sa position et sa situation personnelle.

Dans le cas d'espèce, les hommes qui cherchaient à faire établir leur paternité ne disposaient d'aucune possibilité effective de contester la filiation établie par reconnaissance et aucune possibilité d'établir directement leur propre paternité. Cette situation résultait de la volonté du législateur bulgare, dans un objectif de stabilité des relations familiales, de privilégier la filiation déjà établie par rapport à la possibilité d'établir une paternité biologique. S'il est bien entendu raisonnable de la part des autorités internes de tenir compte du fait que l'enfant ait déjà une filiation établie, la Cour considère que d'autres éléments auraient dû être pris en considération dans ce type de situations. Or, pour rejeter les actions introduites par ces requérants, les juridictions internes, en application des dispositions pertinentes en la matière du Code de la famille, se sont fondées uniquement sur le fait qu'une reconnaissance de paternité avait été effectuée, sans prendre en compte les circonstances particulières de chaque espèce et la situation des différents protagonistes – l'enfant, la mère, le père légitime et le père biologique présumé[48], ce qui n'est pas admissible.

3. *Les délais de prescription*

La Cour a eu connaître d'un cas où les enfants n'avaient pas pu engager d'action en recherche de paternité dans le délai prévu puisque le délai légal d'un an pour agir commençait à courir le jour de leur naissance – outre le fait qu'ils ne connaissaient pas l'identité de leur père. La fixation du délai de prescription, tel qu'il a produit ses effets en l'espèce, a restreint le droit des intéressés à engager des actions en recherche de paternité au point d'éteindre ce droit. Or, les délais de prescription rigides ou

[48] Cour eur. D.H., arrêt du 8 décembre 2016, *L.D. et P.K. c. Bulgarie*, n^os^ 7949/11 et 45522/13, §§ 62, 63 et 75.

d'autres obstacles aux actions en recherche de paternité qui s'appliquent même si les intéressés n'ont pas connaissance de l'identité de leur père présumé avant l'écoulement du délai de prescription méconnaissent l'article 8 de la Convention[49].

G. Vie privée, réputation et liberté d'expression

1. *La vie privée et la protection contre la divulgation d'informations*

La notion de « vie privée » est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne et peut donc englober de multiples aspects de l'identité d'un individu, tels son nom, sa photographie ou des éléments se rapportant au droit à l'image, son intégrité physique et morale, ainsi que des informations dont les individus sont légitimement en droit de s'attendre à ce qu'elles ne soient pas publiées sans leur consentement. La publication d'une photo interfère dès lors avec la vie privée d'une personne, même si cette personne est une personne publique[50].

2. *La vie privée et la protection de la réputation*

Le concept de « vie privée » est une notion large qui n'est pas susceptible d'une définition exhaustive, qui comprend l'intégrité morale d'une personne et peut en conséquence englober plusieurs aspects de son identité comme l'identification et l'orientation sexuelle, le nom ou d'autres éléments relatifs au droit à l'image de la personne. Le droit à la protection de la réputation est un droit protégé comme partie intégrante du droit au respect de la vie privée. La réputation d'une personne, même critiquée dans le contexte d'un débat public, fait partie de son identité personnelle et de son intégrité psychologique. L'attaque à l'honneur et à la réputation doit atteindre un certain degré de gravité et être susceptible de causer un dommage à la jouissance de la personne du droit au respect de la vie privée. La confusion et le mélange entre l'identité sexuelle et l'orientation sexuelle d'une personne dans une émission télévisée humoristique représentent une atteinte suffisamment grave dès lors que cela touche à deux caractéristiques intimes de tout individu[51].

En tout cas, on ne peut pas invoquer la protection de l'article 8 de la Convention pour se plaindre d'une perte de réputation qui est la conséquence prévisible de son propre comportement comme la commission d'une infraction pénale[52].

---

[49] Cour eur. D.H., 19 juillet 2016, *Calin et autres c. Roumanie*, n^os^ 25057/11, 34739/11 et 20316/12, §§ 93-4, 98 et 99.
[50] Cour eur. D.H., arrêt du 17 mars 2016, *Kahn c. Allemagne*, n° 16313/10, § 63 ; Cour eur. D.H., décision du 19 avril 2016, *X c. Saint Marin*, n° 76795/13, § 24 ; Cour eur. D.H., arrêt du 29 mars 2016, *Bédat c. Suisse*, n° 56925/08 (publication par un journaliste d'informations relatives à une procédure pénale en cours liée au drame du Grand-Pont de Lausanne en 2013) (voy. aussi les deux opinions dissidentes).
[51] Cour eur. D.H., arrêt du 22 mars 2016, *Sousa Goucha c. Portugal*, n° 70434/12, §§ 23, 24, 25 et 27. Sur la gravité de l'ingérence, voy. aussi Cour eur. D.H., décision du 19 avril 2016, *X c. Saint Marin*, n° 76795/13, § 24 et la décision du 31 mai 2016, *Yarushkevych c. Ukraine*, n° 38320/05 (§§ 23 et 25). À propos de la protection de la réputation contre une publication relative à l'état de santé mental du requérant qui est un expert en psychologie près les tribunaux, voy. l'arrêt du 17 mai 2016, *Fürst-Pfeifer c. Autriche*, n^os^ 33677/10 et 52340/10.
[52] Cour eur. D.H., décision du 31 mai 2016, *Yarushkevych c. Ukraine*, n° 38320/05, § 25.

3. *La balance entre la liberté d'expression et le droit à la protection de la réputation sous l'angle du droit au respect de la vie privée*

Afin d'apprécier la balance entre la liberté d'expression et le droit à la protection de la réputation sous l'angle du droit au respect de la vie privée, il faut tenir compte des critères suivants[53] :

1° la contribution à un débat d'intérêt public ;

2° le degré de notoriété de la personne concernée ;

3° le sujet du reportage ;

4° le comportement antérieur de la personne concernée ;

5° le contenu, la forme et les conséquences de la publication ;

6° et, le cas échéant, les circonstances dans lesquelles les photographies ont été prises.

En outre, quand la requête est introduite sous le couvert de l'article 10 de la Convention[54], il faut encore prendre en considération[55] :

1° la manière dont l'information a été obtenue ;

2° la véracité de l'information ;

3° la sévérité de la pénalité infligée aux journalistes ou à l'éditeur.

4. *Liberté d'expression et atteinte à l'honneur et à la réputation*

a. Les restrictions à la liberté d'expression

L'article 10, § 2, de la Convention ne laisse guère de place pour des restrictions à la liberté d'expression dans le domaine du discours et du débat politiques (dans lequel la liberté d'expression revêt la plus haute importance) ou des questions d'intérêt général[56].

[53] Cour eur. D.H., décision du 15 mars 2016, *Verlagsgruppe Handelsblatt Gmbh & CO. KG c. Allemagne*, n° 52205/11, § 23.
[54] La justification des ingérences dans la liberté d'expression et la protection de la réputation sous cet angle (§§ 43 et s.) ; Cour eur. D.H., arrêt du 2 juin 2016, *Instytut Ekonomichnykh Reform, Tov c. Ukraine*, n° 61561/08.
[55] Cour eur. D.H., décision du 15 mars 2016, *Verlagsgruppe Handelsblatt Gmbh & CO. KG c. Allemagne*, n° 52205/11, § 23.
[56] Cour eur. D.H., arrêt du 30 août 2016, *Medipress-Sociedade Jornalistica Lda c. Portugal*, n° 55442/12, § 35.

b. La critique admissible à l'égard d'une personne publique

Les limites de la critique admissible sont plus larges à l'égard d'un homme politique, visé en cette qualité, que d'un simple particulier. En effet, à la différence du second, le premier s'expose inévitablement et consciemment à un contrôle attentif de ses faits et gestes tant par les journalistes que par la masse des citoyens. Il doit, par conséquent, montrer une plus grande tolérance. Par ailleurs, la liberté journalistique comprend aussi le recours possible à une certaine dose d'exagération, voire même de provocation[57].

c. Les « devoirs et responsabilités » de la presse

Si la presse ne doit pas franchir certaines limites, tenant notamment à la protection de la réputation et des droits d'autrui, il lui incombe néanmoins de communiquer, dans le respect de ses devoirs et de ses responsabilités, des informations et des idées sur toutes les questions d'intérêt général. Ainsi, la mission d'information comporte nécessairement des « devoirs et des responsabilités » ainsi que des limites que les organes de presse doivent s'imposer spontanément. La Cour rappelle également que la protection offerte aux journalistes par l'article 10 de la Convention est subordonnée à la condition qu'ils agissent de bonne foi de manière à fournir des informations exactes et dignes de crédit dans le respect des principes d'un journalisme responsable[58].

d. La mise en balance des intérêts en jeu

Lorsqu'elle est appelée à se prononcer sur un conflit entre deux droits également protégés par la Convention, la Cour doit effectuer une mise en balance des intérêts en jeu. L'issue de la requête ne saurait en principe varier selon qu'elle a été portée devant elle, sous l'angle de l'article 8 de la Convention, par la personne faisant l'objet de la publication ou, sous l'angle de l'article 10, par son auteur. En effet, ces droits méritent *a priori* un égal respect. Dès lors, la marge d'appréciation devrait en principe être la même dans les deux cas[59].

e. La distinction entre « déclaration de fait » et « jugement de valeur »

La Cour rappelle la distinction qu'elle opère entre « déclaration de fait » et « jugement de valeur ». La matérialité des déclarations de fait peut se prouver. En revanche, les jugements de valeur ne se prêtent pas à une démonstration de leur exactitude. En conséquence, il n'est pas possible d'en rapporter la preuve et l'obligation de le faire porterait atteinte à la liberté d'opinion elle-même qui est un élément fondamental du droit garanti par l'article 10 de la Convention. Cepen-

[57] *Ibid.*, § 36.
[58] *Ibid.*, § 37.
[59] *Ibid.*, § 38.

dant, en présence d'un jugement de valeur, la proportionnalité de l'ingérence dépend de l'existence d'une « base factuelle » suffisante sur laquelle reposeraient les propos litigieux. À défaut, ce jugement de valeur pourrait se révéler excessif. Pour distinguer une imputation de fait d'un jugement de valeur, il faut tenir compte des circonstances de l'espèce et de la tonalité générale des propos, étant entendu que des assertions sur des questions d'intérêt public peuvent constituer à ce titre des jugements de valeur plutôt que des déclarations de fait[60].

f. La marge d'appréciation

Si la mise en balance par les autorités nationales s'est faite dans le respect des critères établis par la jurisprudence de la Cour, il faut des raisons sérieuses pour que celle-ci substitue son avis à celui des juridictions internes. Dans le cas d'espèce, la Cour avait constaté que l'article litigieux avait été publié dans un magazine jouissant d'une certaine crédibilité auprès du public et qu'il portait sur un sujet d'intérêt général relevant de la vie politique et sociale du pays. La marge d'appréciation dont disposaient les autorités pour juger de la nécessité de la condamnation prononcée contre la requérante au civil était, en conséquence, étroite. Cela étant, la Cour rappelle que l'article 10 de la Convention ne garantit pas une liberté d'expression sans aucune restriction même quand il s'agit de rendre compte dans la presse de questions sérieuses d'intérêt général. L'exercice de cette liberté comporte des « devoirs et responsabilités » qui peuvent revêtir de l'importance lorsque, comme en l'espèce, l'on risque de porter atteinte à la réputation de particuliers et de mettre en péril les « droits d'autrui ». Ainsi, l'information rapportée sur des questions d'intérêt général est subordonnée à la condition que les intéressés agissent de bonne foi de manière à fournir des informations exactes et dignes de crédit. La Cour rappelle que, s'il est vrai que les adversaires des idées et positions officielles doivent pouvoir trouver leur place dans l'arène politique, discutant au besoin des actions menées par des responsables dans le cadre de l'exercice de leurs mandats publics, ils sont également tenus de ne pas dépasser certaines limites quant au respect (notamment) de la réputation et des droits d'autrui[61].

5. *La sanction pour la publication de photographies*

On ne peut pas tirer de l'article 8 de la Convention le principe selon lequel, pour protéger la vie privée d'une personne de manière effective, la condamnation d'un éditeur au paiement d'une somme pour avoir enfreint une interdiction de publier ne saurait être suffisante que si cette somme revient à la victime, si tant est que l'État, dans l'exercice de sa marge d'appréciation qui lui revient dans ce domaine, met à la disposition des personnes lésées d'autres moyens qui peuvent se révéler

[60] *Ibid.*, § 39.
[61] *Ibid.*, §§ 40-42. À propos de la publication de photographies nues, voy. la décision du 8 novembre 2016 (*Mertinas et Mertiniene c. Lituanie*, n° 43579/09).

effectifs et dont on ne saurait dire qu'ils limitent la possibilité d'obtenir le redressement des violations alléguées de manière disproportionnée[62].

Dans l'hypothèse d'une publication d'informations personnelles ou de photographies dans les médias, l'article 8 ne requiert pas nécessairement un recours de nature pénale et les mesures de nature civile sont habituellement suffisantes[63].

H. La responsabilité éditoriale sur les sites web d'information

Même si les portiques d'informations sur l'Internet ne sont pas les éditeurs, au sens traditionnel du terme, des commentaires postés, ils doivent quand même, en principe, supporter des obligations et des responsabilités. En raison de la nature particulière de l'Internet, ces obligations et responsabilités peuvent différer jusqu'à un certain point de celles qui incombent à l'éditeur traditionnel, notamment en ce qui concerne les contenus de tiers[64]. Le système de « *notice-and-take-down* » accouplé à une procédure effective aboutissant à une réaction rapide, constitue dans la plupart des cas un moyen approprié pour la balance des droits et intérêts des parties impliquées, comme pour la protection de la réputation commerciale d'une entreprise (qui ne se confond pas avec la réputation d'une personne physique). Lorsque les commentaires prennent la forme de discours haineux et de menaces directes à l'intégrité physique d'individus, les droits et intérêts d'autrui et de la société peuvent conduire à imposer une responsabilité aux portiques d'information sur l'Internet quand ils sont en défaut de prendre les mesures requises pour enlever sans délai les commentaires illégaux même sans requête de la part de la personne concernée ou d'un tiers[65].

I. Droit d'accès à l'information et/ou aux documents officiels détenus par des organes publics et protection des données à caractère personnel

La Cour estime d'abord que rien ne l'empêche d'interpréter l'article 10, § 1er, de la Convention comme incluant un droit d'accès à l'information[66]. Ensuite, elle indique qu'elle considère toujours que « le droit à la liberté de recevoir des informations interdit essentiellement à un gouvernement d'empêcher quelqu'un de recevoir des informations que d'autres aspirent ou peuvent consentir à lui fournir » et que « le droit de recevoir des informations ne saurait se comprendre comme imposant à un État des obligations positives de collecte et de diffusion, *motu proprio*, des informations ». La Cour considère donc que l'article 10 n'accorde pas à l'individu un droit

[62] Cour eur. D.H., arrêt du 17 mars 2016, *Kahn c. Allemagne*, n° 16313/10, § 75.
[63] Cour eur. D.H., décision du 4 octobre 2016, *A.C. c. Lituanie*, n° 59076/08, § 46.
[64] Cour eur. D.H., arrêt du 2 février 2016, *Magyar Tartalomszolgaltatok Egyeysülete & Index.hu Zrt c. Hongrie*, n° 22947/13, § 62.
[65] *Ibid.*, § 91.
[66] Cour eur. D.H. (GC), arrêt du 8 novembre 2016, *Magyar Helsinki Bizottsag c. Hongrie*, n° 18030/11, § 149.

d'accès aux informations détenues par une autorité publique, ni n'oblige l'État à les lui communiquer. Toutefois, un tel droit ou une telle obligation peut naître, premièrement, lorsque la divulgation des informations a été imposée par une décision judiciaire devenue exécutoire et, deuxièmement, lorsque l'accès à l'information est déterminant pour l'exercice par l'individu de son droit à la liberté d'expression, en particulier « la liberté de recevoir et de communiquer des informations » et que refuser cet accès constituerait une ingérence dans l'exercice de ce droit.

La question de savoir si, et dans quelle mesure, le refus de donner accès à des informations a constitué une ingérence dans l'exercice par un requérant du droit à la liberté d'expression doit s'apprécier au cas par cas à la lumière des circonstances particulières de la cause. Les critères pertinents à prendre en compte sont les suivants[67] :

1° le but de la demande d'information, la nature des informations recherchées ;

2° le rôle de la personne qui recherche l'information ;

3° et les informations déjà disponibles.

À propos de la divulgation de données à caractère personnel relatives aux avocats commis d'office dont la requérante avait besoin pour son étude sur l'efficacité de ces derniers, la Cour a noté que si les noms des avocats commis d'office étaient bien des données à caractère personnel, la demande de leur communication se rapportait principalement à la conduite d'activités professionnelles dans le cadre de procédures publiques. En ce sens, les activités professionnelles des avocats commis d'office ne pouvaient pas être considérées comme étant une question privée.

De plus, les informations recherchées n'avaient pas trait aux actions ou aux décisions de ces avocats dans le cadre de l'accomplissement de leur tâche de conseil juridique ni à leurs consultations avec leurs clients. Le Gouvernement n'a pas démontré que la divulgation des informations que la requérante avait sollicitées précisément aux fins d'alimenter son enquête, eût pu porter atteinte à la jouissance par les avocats concernés de leur droit au respect de la vie privée au sens de l'article 8 de la Convention.

La Cour considère également que la divulgation du nom des avocats commis d'office et du nombre de fois où chacun d'eux avait été commis n'aurait pas constitué, les concernant, des révélations allant au-delà de ce à quoi ils pouvaient s'attendre en s'inscrivant comme avocats susceptibles d'être commis d'office.

Il n'y a pas de raison de présumer que le public ne pouvait pas prendre connaissance par d'autres moyens du nom des différents avocats commis d'office et du

[67] *Ibid.*, §§ 156-170.

nombre de fois où ils avaient été commis, par exemple en recueillant les informations qui figuraient dans les listes d'avocats disponibles au titre de l'assistance judiciaire ainsi que dans les calendriers des audiences des tribunaux et en assistant aux audiences publiques, même si ces informations n'étaient pas réunies au même endroit au moment de l'étude.

Dans ce contexte, les intérêts invoqués par le Gouvernement, qui se réfère à l'article 8 de la Convention, ne sont pas d'une nature et d'un degré propres à justifier l'application de cette disposition et leur mise en balance avec le droit de la requérante découlant de l'article 10, § 1er, de la Convention. Néanmoins, l'article 10 ne garantit pas une liberté d'expression illimitée et la protection des intérêts privés des avocats commis d'office constitue un but légitime permettant de restreindre la liberté d'expression. Ainsi, la question essentielle à trancher est celle de savoir si les moyens employés pour protéger ces intérêts étaient proportionnés au but visé.

En l'espèce, la Cour a considéré qu'il n'y aurait pas eu d'atteinte au droit au respect de la vie privée des avocats commis d'office si la demande d'information de la requérante avait été acceptée. Même s'il est vrai que cette demande concernait des données à caractère personnel, elle ne portait pas sur des informations se trouvant hors du domaine public. Il s'agissait seulement d'informations de nature statistique sur le nombre de fois où chacune des personnes en question avait été désignée pour représenter un accusé dans une procédure pénale publique dans le cadre du dispositif national d'assistance judiciaire financé par l'État.

Toujours dans le cas d'espèce, le droit hongrois pertinent, tel qu'interprété par les juridictions internes compétentes, excluait toute appréciation sérieuse du respect du droit de la requérante à la liberté d'expression. Or, toute restriction à la démarche de l'intéressée visant à publier l'étude en question (qui avait pour but de contribuer à un débat sur une question d'intérêt général) aurait dû faire l'objet d'un contrôle minutieux.

La Cour a, en conséquence, considéré que les arguments avancés par le Gouvernement étaient pertinents mais non suffisants pour démontrer que l'ingérence dénoncée était « nécessaire dans une société démocratique ». En particulier, elle a jugé que, nonobstant la marge d'appréciation de l'État, il n'y avait pas de rapport raisonnable de proportionnalité entre la mesure litigieuse et le but légitime poursuivi[68].

[68] Cour eur. D.H. (GC), arrêt du 8 novembre 2016, *Magyar Helsinki Bizottsag c. Hongrie*, nº 18030/11, §§ 194-196, 198, 199 et 200.

II. La protection des données dans la jurisprudence du Tribunal et de la Cour de justice de l'Union européenne

A. Le champ d'application territorial de la directive 95/46/CE

La Cour a été saisie d'une question préjudicielle portant sur la détermination de la loi applicable en matière de protection des données à caractère personnel dans le cadre d'un contrat conclu par voie électronique avec des consommateurs[69]. Dans ce contexte, la Cour a procédé à une analyse de l'article 4.1.a de la directive 95/46 qui précise que « le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable »[70]. Elle a rappelé que la notion d'établissement « s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable (arrêt du 1er octobre 2015, *Weltimmo*, aff. C-230/14, EU:C:2015:639, point 31) »[71] et que la circonstance que l'entreprise concernée « ne possède ni filiale ni succursale dans un État membre n'exclut pas qu'elle puisse y posséder un établissement au sens de l'article 4, paragraphe 1er, sous a), de la directive 95/46 »[72].

Cependant et considérant qu'« il convient plutôt d'évaluer, ainsi que la Cour l'a déjà relevé, tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans l'État membre en question (voy., en ce sens, arrêt du 1er octobre 2015, *Weltimmo*, aff. C-230/14, EU:C:2015:639, point 29) »[73], la Cour a précisé que l'« établissement ne saurait exister du simple fait que le site Internet de l'entreprise en question y est accessible »[74]. Au terme de son analyse, elle a jugé que « l'article 4, paragraphe 1er, sous a), de la 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, doit être interprété en ce sens qu'un traitement de données à caractère personnel effectué par une entreprise de commerce électronique est régi par le droit de l'État membre vers lequel cette entreprise dirige ses activités s'il s'avère que cette entreprise procède au traitement des données en question dans le cadre des activités d'un établissement situé dans cet État membre »[75] et qu'« il appartient à la juridiction nationale d'apprécier si tel est le cas »[76].

---

[69] C.J.U.E., 28 juin 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, aff. C-191/15.
[70] Directive 95/46 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, article 4.1.a.
[71] C.J.U.E., *Verein für Konsumenteninformation c. Amazon EU Sàrl*, § 75.
[72] *Ibid.*, § 76.
[73] *Ibid.*, § 77.
[74] *Ibid.*, § 76.
[75] *Ibid.*, dispositif.
[76] *Ibid.*

Il est utile de relever que le RGPD définit la notion d'« établissement principal »[77] en donnant des critères d'évaluation, au contraire de la directive 95/46 qui laissait, en fin de compte, la porte ouverte à diverses interprétations.

B. La notion de donnée à caractère personnel

La Cour a été saisie d'une question préjudicielle portant sur l'interprétation à donner à la notion de donnée à caractère personnel définie à l'article 2.a de la directive 95/46 comme étant « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[78]. Le cas concernait un litige opposant Monsieur Breyer à la République fédérale d'Allemagne relatif à « l'enregistrement et de la conservation par cette dernière de l'adresse de protocole Internet (ci-après l' "adresse IP") de M. Breyer lors de la consultation par celui-ci de plusieurs sites Internet des services fédéraux allemands »[79]. La juridiction de renvoi s'interrogeait sur le fait de savoir si une adresse IP dynamique devait être considérée comme une donnée à caractère personnel.

Dans un premier temps, la Cour a d'abord rappelé l'enseignement contenu dans l'arrêt *Scarlet Extended* dans lequel elle avait considéré que « les adresses IP des utilisateurs d'Internet étaient des données protégées à caractère personnel, car elles permettent l'identification précise de ces utilisateurs »[80] tout en précisant que cet arrêt concernait la « collecte et l'identification des adresses IP des utilisateurs d'Internet effectuées par les fournisseurs d'accès à Internet »[81]. Elle a, ensuite, précisé que les adresses IP dynamiques ne se rapportaient pas à des personnes identifiées « dans la mesure où une telle adresse ne révèle pas directement l'identité de la personne physique propriétaire de l'ordinateur à partir duquel la consultation d'un site Internet a lieu ni celle d'une autre personne qui pourrait utiliser cet ordinateur »[82]. Au terme de cette première étape, la Cour s'est attachée à déterminer si de telles adresses se rapportaient à des personnes identifiables. À cet effet, elle a rappelé le considérant 26 de la directive qui « fait référence aux moyens susceptibles d'être raisonnablement mis en œuvre tant par le responsable du traitement que par une "autre personne" »[83], ce qui implique donc qu'« il n'est pas requis que toutes les informations permettant d'identifier la personne concernée doivent se trouver entre les mains d'une seule personne »[84].

[77] Voy. article 4.16 du RGPD.
[78] C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14.
[79] *Ibid.*, § 2.
[80] *Ibid.*, § 33.
[81] *Ibid.*, § 34.
[82] *Ibid.*, § 38.
[83] *Ibid.*, § 43.
[84] *Ibid.*

Elle a également repris un argument de l'Avocat général qui avait précisé que les moyens mis en œuvre ne pouvaient pas être considérés comme raisonnables « si l'identification de la personne concernée était interdite par la loi ou irréalisable en pratique, par exemple en raison du fait qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main-d'œuvre, de sorte que le risque d'une identification paraît en réalité insignifiant »[85]. La Cour s'est ainsi interrogée sur la possibilité de combiner les adresses IP et des informations complémentaires permettant d'identifier la personne concernée et a conclu que « le fournisseur de services de médias en ligne dispose de moyens susceptibles d'être raisonnablement mis en œuvre afin de faire identifier, à l'aide d'autres personnes, à savoir l'autorité compétente et le fournisseur d'accès à Internet, la personne concernée sur la base des adresses IP conservées »[86].

Au terme de son analyse, la juridiction européenne a considéré que « l'article 2, sous a), de la directive 95/46 doit être interprété en ce sens qu'une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne »[87]. La Cour précise ainsi que les moyens légaux à disposition du responsable du traitement constituent un critère complémentaire pour déterminer si des moyens sont ou non raisonnables dans le cadre de l'identification de la personne concernée.

C. La légitimation des traitements de données

Toujours dans l'affaire *Patrick Breyer c. Bundesrepublik Deutschland*, la Cour devait également répondre à une seconde question préjudicielle relative à la base de légitimation utilisée pour la collecte et l'enregistrement des adresses IP telle que prévue à l'article 7.f de la directive 95/46, soit lorsque le traitement de données 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, qui appellent une protection au titre de l'article 1er, paragraphe 1er [de la directive 95/46] ».

La Cour a eu l'occasion de rappeler que cette disposition « s'oppose à une réglementation d'un État membre en vertu de laquelle un fournisseur de services de médias en ligne ne peut collecter et utiliser des données à caractère personnel afférentes à un utilisateur de ces services, en l'absence du consentement de celui-ci,

[85] *Ibid.*, § 46.
[86] *Ibid.*, § 48.
[87] *Ibid.*, § 49.

que dans la mesure où cette collecte et cette utilisation sont nécessaires pour permettre et facturer l'utilisation concrète desdits services par cet utilisateur, sans que l'objectif visant à garantir la capacité générale de fonctionnement des mêmes services puisse justifier l'utilisation desdites données après une session de consultation de ceux-ci »[88].

En l'espèce, la loi allemande sur les médias en ligne disposait que la collecte et l'utilisation des données à caractère personnel par le fournisseur de services n'étaient autorisées que pour permettre et facturer l'utilisation des médias en ligne, ce que la Cour a considéré comme contraire à la directive 95/46 en ce que cette loi était plus restrictive que l'article 7.f de la directive[89]. En effet, les fournisseurs de service qui « fournissent des services de médias en ligne pourraient également avoir un intérêt légitime à garantir, au-delà de chaque utilisation concrète de leurs sites Internet accessibles au public, la continuité du fonctionnement desdits sites »[90].

D. La conservation des données

Dans un arrêt du 21 décembre 2016[91], la Cour a eu l'occasion d'analyser la question de la conservation des données à caractère personnel imposée aux fournisseurs de services de communications électroniques. Elle a ainsi précisé que « l'article 15, paragraphe 1er, de la directive 2002/58 [directive e-privacy], lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1er, de la Charte [des droits fondamentaux de l'Union européenne], doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique », tout en précisant que cette même lecture « ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire »[92].

Elle a poursuivi son raisonnement en précisant que :

> « Pour satisfaire [ces exigences, la] réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent

[88] *Ibid.*, § 64.
[89] *Ibid.*, § 59.
[90] *Ibid.*, § 60.
[91] C.J.U.E., *Tele2 Sverige AB c. Post-och telestyrelsen*, aff. C-203/15 et C-698/15.
[92] *Ibid.*, § 108.

> de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voy., par analogie, à propos de la directive 2006/24, arrêt *Digital Rights*, point 54 et jurisprudence citée).
>
> En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné »[93].

Il est intéressant de relever que la proposition de règlement européen concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques ») prévoit que « les États membres sont libres de maintenir ou de créer, en la matière, des cadres nationaux qui prévoient, entre autres, des mesures de conservation ciblées dans la mesure où ces cadres respectent le droit de l'Union, compte tenu de la jurisprudence de la Cour de justice sur l'interprétation de la directive "vie privée et communications électroniques" et de la Charte [des droits fondamentaux de l'Union européenne] »[94]. Par jurisprudence de la Cour de justice, la Commission vise expressément l'arrêt *Tele2 Sverige AB c. Post-och telestyrelsen*.

E. Le droit d'accès par les autorités

Encore dans ce même arrêt, la Cour a fixé des règles concernant l'accès des autorités aux données stockées par les fournisseurs de services de communications électroniques, en précisant que :

> « Un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire, la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits.

[93] *Ibid.*, §§ 109 et 110.
[94] Proposition de règlement européen concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), 2017/0003, 10 janvier 2017, p. 3.

> À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction (voy., par analogie, Cour eur. D.H., 4 décembre 2015, *Zakharov c. Russie*, CE:ECHR:2015:1204JUD004714306, § 260). Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités ».

La Cour en a conclu que :

> « L'article 15, paragraphe 1er, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1er, de la Charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union »[95].

Jean Herveg

Directeur de Recherche au Centre de Recherches Information, Droit et Société.
Avocat au barreau de Bruxelles.
Auteur de la partie consacrée à la Cour européenne des droits de l'homme.

Jean-Marc Van Gyseghem

Directeur de Recherche au Centre de Recherches Information, Droit et Société.
Avocat au barreau de Bruxelles.
Auteur de la partie consacrée aux juridictions de l'Union européenne.

[95] *Ibid.*, dispositif.