



décembre 2022

Cette fiche ne lie pas la Cour et n'est pas exhaustive

# Protection des données personnelles

« Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'**article 8 [de la Convention européenne des droits de l'homme]** qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance<sup>1</sup> (...). Peu importe que les informations mémorisées soient ou non utilisées par la suite (...). Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu [un aspect] de la vie privée (...), la Cour [européenne des droits de l'homme] tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés (...). » (*S. et Marper c. Royaume-Uni*, arrêt (Grande Chambre) du 4 décembre 2008, § 67)

## Collecte de données personnelles

### Données ADN et empreintes digitales

Voir ci-dessous, sous « Conservation et exploitation des données personnelles », « Dans le contexte de la police et de la justice pénale ».

### Données GPS

#### Uzun c. Allemagne

2 septembre 2010

Le requérant, soupçonné d'avoir participé à des attentats à la bombe perpétrés par un mouvement d'extrême gauche, alléguait que sa surveillance par GPS et l'utilisation des données ainsi obtenues dans le cadre de la procédure pénale dirigée contre lui avaient emporté violation de son droit au respect de sa vie privée.

La Cour a conclu en l'espèce à la **non-violation de l'article 8** de la Convention. Certes, la surveillance du requérant par GPS ainsi que le traitement et l'utilisation des données ainsi obtenues s'analysaient en une ingérence dans l'exercice par l'intéressé de son droit au respect de sa vie privée. Toutefois, a noté la Cour, cette ingérence poursuivait des buts légitimes, à savoir la protection de la sécurité nationale, de la sûreté publique et des droits des victimes, ainsi que la prévention des infractions pénales. Elle était également proportionnée : la surveillance par GPS avait seulement été ordonnée après que d'autres mesures d'investigation, moins attentatoires à la vie privée, se furent révélées moins efficaces, et cette mesure avait été mise en œuvre pendant une période relativement courte (quelque trois mois) et n'avait touché l'intéressé que lorsqu'il se déplaçait dans la voiture de son complice. Dès lors, on ne saurait dire que le requérant

<sup>1</sup> L'article 8 de la [Convention européenne des droits de l'homme](#) dispose que :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.  
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

avait été soumis à une surveillance totale et exhaustive. L'enquête ayant porté sur des infractions très graves, la Cour a donc jugé que la surveillance de l'intéressé par GPS avait été nécessaire dans une société démocratique.

### **Ben Faiza c. France**

8 février 2018

Cette affaire concernait des mesures de surveillance prises à l'encontre du requérant dans le cadre d'une enquête pénale portant sur un trafic de stupéfiants. L'intéressé se plaignait que ces mesures – mise en place d'un dispositif de géolocalisation sur son véhicule et réquisition à un opérateur de téléphonie pour recueillir les appels entrants et sortants mais également « bornage » de lignes téléphoniques, permettant de suivre *a posteriori* ses déplacements – avaient constitué une ingérence dans sa vie privée.

La Cour a conclu à la **violation de l'article 8** de la Convention en ce qui concerne la mesure de géolocalisation en temps réel du 3 juin 2010 par apposition d'un récepteur GPS sur le véhicule du requérant, jugeant que, dans le domaine des mesures de géolocalisation en temps réel, le droit français, écrit et non écrit, n'indiquait pas, au moment des faits, avec assez de clarté, l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités. Le requérant n'avait dès lors pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique. La Cour a cependant pris note que par la suite la France s'est dotée d'un dispositif législatif encadrant le recours à la géolocalisation et renforçant la protection du droit au respect de la vie privée (loi du 28 mars 2014). La Cour a par ailleurs conclu à l'**absence de violation de l'article 8** concernant la réquisition judiciaire adressée à un opérateur de téléphonie mobile le 24 juillet 2009 pour obtenir la liste des bornes déclenchées par la ligne téléphonique du requérant afin de retracer *a posteriori* ses déplacements. Elle a relevé à cet égard que la réquisition judiciaire avait constitué une ingérence dans la vie privée du requérant mais que celle-ci était prévue par la loi. Visant en outre à permettre la manifestation de la vérité dans le cadre d'une procédure pénale relative à des faits d'importation de stupéfiants en bande organisée, d'association de malfaiteurs et de blanchiment, la réquisition judiciaire avait poursuivi un but légitime, à savoir la défense de l'ordre, la prévention des infractions pénales ainsi que la protection de la santé publique. La Cour a également estimé que cette mesure avait été nécessaire dans une société démocratique car elle avait visé à démanteler un trafic de stupéfiants de grande ampleur. Enfin, les informations obtenues par ce biais avaient été utilisées dans le cadre d'une enquête et d'un procès pénal au cours duquel le requérant avait bénéficié d'un contrôle effectif tel que voulu par la prééminence du droit.

### **Florindo de Almeida Vasconcelos Gramaxo c. Portugal**

13 décembre 2022<sup>2</sup>

Cette affaire portait sur le licenciement du requérant sur la base de données recueillies à partir d'un système de géolocalisation installé sur le véhicule que son employeur avait mis à sa disposition afin d'exercer ses fonctions de délégué médical. Le requérant soutenait notamment que le traitement de données de géolocalisation obtenues à partir du système GPS installé sur son véhicule de fonction et l'utilisation de ces données pour fonder son licenciement avaient porté atteinte à son droit au respect de sa vie privée. Il se plaignait également d'un manque d'équité de la procédure menée devant les juridictions nationales, au motif que celles-ci se seraient fondées presque exclusivement sur des preuves illicites recueillies au moyen du système GPS installé dans son véhicule de fonction.

La Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que les autorités portugaises n'avaient pas manqué à l'obligation positive qui leur incombait de protéger le droit du requérant au respect de sa vie privée. Elle a observé tout d'abord que le requérant savait que l'entreprise avait installé un système GPS sur son véhicule dans le but de contrôler les kilomètres parcourus dans l'exercice de son activité

---

<sup>2</sup>. Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 (arrêts définitifs) de la [Convention européenne des droits de l'homme](#).

professionnelle et, le cas échéant, lors de ses déplacements privés. Elle a noté ensuite qu'en ne retenant que les données de géolocalisation concernant le kilométrage parcouru, la cour d'appel avait réduit l'ampleur de l'intrusion dans la vie privée du requérant à ce qui était strictement nécessaire au but légitime poursuivi, à savoir le contrôle des dépenses de l'entreprise. En l'espèce, la Cour a estimé que la cour d'appel avait mis en balance de manière circonstanciée le droit du requérant au respect de sa vie privée et le droit de son employeur au bon fonctionnement de l'entreprise, en tenant compte du but légitime qui était poursuivi par l'entreprise, à savoir le droit de veiller au contrôle de ses dépenses. La marge d'appréciation qui revenait à l'État dans le cas présent n'avait donc pas été dépassée. La Cour a également conclu à **non-violation de l'article 6 § 1** (droit à un procès équitable) de la Convention, jugeant que l'utilisation comme preuves des données de géolocalisation relatives au kilométrage parcouru par le requérant dans son véhicule de fonction n'avait pas porté atteinte à l'équité de la procédure dans la présente affaire.

## Données médicales

### L.H. c. Lettonie (n° 52019/07)

29 avril 2014

La requérante alléguait en particulier que la collecte par un organisme d'État (en l'espèce, l'inspection du contrôle de la qualité des soins médicaux et de l'aptitude au travail (« MADEKKI »)) de ses données médicales personnelles, sans son consentement, avait violé son droit au respect de sa vie privée.

La Cour a rappelé dans cet arrêt l'importance de la protection des données médicales pour la jouissance par une personne du droit au respect de sa vie privée. Dans le cas de la requérante, elle a conclu à la **violation de l'article 8** de la Convention, jugeant que le droit applicable ne définissait pas avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes. En particulier, la Cour a observé que le droit letton ne limitant aucunement la portée des données personnelles pouvant être recueillies par le MADEKKI, celui-ci avait réuni en ce qui concerne la requérante des informations médicales se rapportant à une période de sept ans, et ce sans distinction et sans appréciation préalable du point de savoir si ces éléments pouvaient être déterminants, pertinents ou importants pour atteindre le but poursuivi par l'enquête en question.

### Y.G. c. Russie (n° 8647/12)<sup>3</sup>

30 août 2022<sup>4</sup>

Voir ci-dessous, sous « Divulgateion de données personnelles ».

## Données reflétant l'orientation sexuelle

### Drelon c. France

8 septembre 2022<sup>5</sup>

Cette affaire (deux requêtes) portait, d'une part, sur la collecte et la conservation, par l'Établissement français du sang, de données personnelles reflétant l'orientation sexuelle supposée du requérant ainsi que le rejet, par les juridictions pénales, de la plainte pour discrimination qu'il avait déposée et, d'autre part, sur les refus opposés à ses candidatures au don du sang ainsi que sur le rejet, par le Conseil d'État, de son recours pour excès de pouvoir dirigé contre l'arrêté du 5 avril 2016 modifiant les critères de sélection des candidats au don de sang.

La Cour a conclu à la **violation de l'article 8** de la Convention en raison de la collecte et de la conservation des données personnelles litigieuses. S'agissant de la première

<sup>3</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention européenne des droits de l'homme (« la Convention »).

<sup>4</sup>. Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 de la [Convention](#).

<sup>5</sup>. Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 de la [Convention](#).

requête, elle a considéré que la collecte et la conservation de données personnelles sensibles avaient constitué une ingérence dans le droit au respect de la vie privée du requérant. La Cour a jugé que cette ingérence était fondée sur une base légale prévisible, le pouvoir d'appréciation laissé aux autorités concernant la création de fichier de santé étant, en la matière, suffisamment encadré par la loi du 6 janvier 1978 alors applicable. Après avoir considéré que la collecte et la conservation de données personnelles relatives aux résultats des procédures de sélection des candidats au don du sang contribuaient à garantir la sécurité transfusionnelle, elle a précisé que, pour autant, il était particulièrement important que les données sensibles concernées par ce traitement soient exactes, mises à jour, adéquates, pertinentes et non excessives par rapport aux finalités poursuivies, et que leur durée de conservation n'excède pas celle qui est nécessaire. Or, la Cour a relevé en premier lieu qu'alors que le requérant avait refusé de répondre aux questions relatives à sa sexualité lors de l'entretien médical préalable au don, le traitement de données avait été renseigné par la contre-indication au don propre aux hommes ayant eu un rapport sexuel avec un homme. Elle en a déduit que les données collectées, fondées sur de simples spéculations, n'avaient reposé sur aucune base factuelle avérée. En second lieu, après avoir relevé que le gouvernement français n'avait pas démontré que la durée de conservation des données litigieuses (jusqu'en 2278 à l'époque des faits litigieux) était encadrée de telle sorte qu'elle ne puisse pas excéder celle nécessaire aux finalités pour lesquelles elles avaient été collectées, la Cour a jugé que la durée excessive de conservation des données litigieuses avait rendu possible leur utilisation répétée à l'encontre du requérant, entraînant son exclusion automatique du don de sang. S'agissant de la seconde requête, la Cour a **rejeté** comme tardifs les griefs relatifs aux mesures d'exclusion du don de sang des 16 novembre 2004 et 9 août 2006. En ce qui concerne la mesure du 26 mai 2016, elle a indiqué au requérant qu'il ne pouvait invoquer la violation des articles 8 et 14 (interdiction de la discrimination) de la Convention qu'aurait entraînée la mise en œuvre de l'arrêté du 5 avril 2016 qui n'était pas encore en vigueur à la date du refus qu'il contestait devant elle.

## Échantillons de salive

### **Dragan Petrović c. Serbie**

14 avril 2020

Cette affaire concernait la réalisation d'une perquisition par la police au domicile du requérant et le prélèvement d'un échantillon de salive sur sa personne aux fins d'une analyse ADN dans le cadre d'une enquête pour meurtre. L'intéressé alléguait que la perquisition de son domicile et le prélèvement d'un échantillon de son ADN s'analysaient en une atteinte à ses droits protégés par la Convention

La Cour a conclu à la **non-violation de l'article 8** de la Convention en ce qui concerne la perquisition menée par la police au domicile du requérant, jugeant que le mandat de perquisition était suffisamment précis et assorti de garanties adéquates et effectives propres à prévenir tout abus au cours de la perquisition. Elle a conclu, en revanche, à la **violation de l'article 8** à raison du prélèvement d'un échantillon de salive sur la personne du requérant aux fins d'un test ADN, jugeant que le prélèvement n'était pas « prévu par la loi » au sens de l'article 8. En effet, la version du code de procédure pénale qui était en vigueur en Serbie à l'époque des faits disposait uniquement que des prélèvements sanguins ou « d'autres procédures médicales » pouvaient être réalisés. La Cour a par ailleurs noté que de nouvelles garanties concernant les prélèvements d'échantillons de salive avaient été insérées dans le code de procédure pénale en 2011, ce qui constituait selon elle une reconnaissance implicite de leur absence dans la version antérieure du texte.

## Échantillons vocaux

### **P.G et J.H. c. Royaume-Uni (n° 44787/98)**

25 septembre 2001

Cette affaire concernait notamment l'enregistrement de la voix des requérants – arrêtés car soupçonnés d'être sur le point de commettre un vol – dans les locaux d'un commissariat.

La Cour a conclu à la **violation de l'article 8** de la Convention concernant l'utilisation de dispositifs d'écoute cachés dans les locaux du commissariat. Constatant en particulier qu'il n'existait à l'époque des faits aucun système légal au Royaume-Uni pour réglementer l'usage des dispositifs d'écoute cachés de la part de la police dans ses locaux, elle a jugé que l'ingérence dans le droit des requérants au respect de leur vie privée n'était pas prévue par la loi. Dans cette affaire, la Cour a également conclu à la **violation de l'article 8** en ce qui concerne l'utilisation d'un dispositif d'écoute caché dans un appartement ainsi qu'à la **non-violation de l'article 8** quant à l'obtention d'informations relatives à l'utilisation d'un téléphone.

### **Vetter c. France**

31 mai 2005

À la suite de la découverte du corps d'une personne abattue par arme à feu, la police judiciaire, qui soupçonnait le requérant d'être l'auteur de cet homicide, sonorisa l'appartement d'une personne chez qui celui-ci se rendait régulièrement. Sur la base de l'enregistrement des conversations, le requérant fut arrêté et poursuivi pour les faits d'homicide.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que, dans le domaine de la pose de micros, le droit français n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités pouvant autoriser les écoutes des conversations privées. Le requérant n'avait dès lors pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique.

## Interception de communications, écoutes téléphoniques et opérations secrètes de surveillance

### **Klass et autres c. Allemagne**

6 septembre 1978

Dans cette affaire, les requérants, cinq avocats allemands, dénonçaient en particulier la législation allemande qui permettait aux autorités de surveiller leur correspondance et leurs communications téléphoniques sans qu'elles aient l'obligation de les informer ultérieurement des mesures prises contre eux.

La Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que le législateur allemand était fondé à considérer l'ingérence résultant de la législation litigieuse dans l'exercice du droit consacré par l'article 8 § 1 comme nécessaire, dans une société démocratique, à la sécurité nationale, la défense de l'ordre et la prévention des infractions pénales (article 8 § 2). La Cour a observé en particulier que le pouvoir de surveiller en secret les citoyens, caractéristique de l'État policier, n'était tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques. Constatant toutefois que les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire, elle a estimé que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications était, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales.

### Malone c. Royaume-Uni

2 août 1984

Le requérant, inculpé de plusieurs délits de recel de biens volés, se plaignait en particulier de l'interception de ses communications postales et téléphoniques par ou pour la police ainsi que du « comptage » de son téléphone (emploi d'un mécanisme qui enregistre les numéros formés sur un appareil de téléphone donné ainsi que l'heure et la durée de chaque appel).

La Cour a conclu à la **violation de l'article 8** de la Convention, en ce qui concerne tant l'interception de communications que la livraison de relevés de comptage à la police, dans la mesure où ceux-ci n'étaient pas prévus par la loi.

### Kruslin c. France

24 avril 1990

Cette affaire concernait le placement du requérant sous écoute téléphonique par un juge d'instruction dans le cadre d'une affaire d'assassinat.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que le droit français n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans ce domaine. Il en allait encore davantage ainsi à l'époque des faits de l'espèce, de sorte que la Cour a considéré que le requérant n'avait pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique.

Voir aussi, parmi d'autres : Huvig c. France, arrêt du 24 avril 1990 ; Halford c. Royaume-Uni, arrêt du 25 juin 1997.

### Kopp c. Suisse

25 mars 1998

Cette affaire concernait la mise sur écoute des lignes téléphoniques du cabinet d'avocats du requérant sur instruction du procureur général de la Confédération.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que le droit suisse n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. Elle a dès lors estimé que le requérant, en sa qualité d'avocat, n'avait pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique.

### Amann c. Suisse

16 février 2000 (Grande Chambre)

Cette affaire concernait un appel téléphonique passé au requérant depuis l'ambassade alors soviétique – pour lui commander un appareil dépilatoire qu'il commercialisait – intercepté par le ministère public, qui fit établir sur le requérant une fiche par les services de renseignements.

La Cour a conclu à la **violation de l'article 8** de la Convention concernant tant l'interception de l'appel téléphonique que l'établissement et la conservation de la fiche, estimant que ces ingérences dans la vie privée du requérant n'étaient pas prévues par la loi, le droit suisse étant imprécis quant au pouvoir d'appréciation des autorités dans ce domaine.

### Taylor-Sabori c. Royaume-Uni

22 octobre 2002

Cette affaire concernait en particulier l'interception par la police, dans le cadre d'une opération de surveillance spéciale, de messages envoyés sur le messenger de poche du requérant.

La Cour a conclu à la **violation de l'article 8** de la Convention. Relevant qu'à l'époque des faits, aucune disposition légale ne réglementait l'interception de messages reçus sur des messagers de poche et transmis par l'intermédiaire d'un système de télécommunications privé, elle a jugé, comme le gouvernement britannique l'avait reconnu, que l'ingérence dans la vie privée et la correspondance du requérant n'était pas prévue par la loi.

### **Wisse c. France**

22 décembre 2005

Soupçonnés de commettre des vols avec armes, les requérants furent interpellés et mis en détention provisoire. Sur commission rogatoire, leurs conversations téléphoniques avec leurs proches dans les parloirs furent enregistrées. Les requérants demandèrent vainement l'annulation des actes de procédure relatifs aux enregistrements de leurs conversations dans le parloir. Ils soutenaient que l'enregistrement de leurs conversations dans les parloirs des prisons avait constitué une ingérence dans leur droit au respect de leur vie privée et familiale.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que le droit français n'indiquait pas avec assez de clarté la possibilité d'ingérence par les autorités dans la vie privée des détenus, ainsi que l'étendue et les modalités d'exercice de leur pouvoir d'appréciation dans ce domaine. Les requérants n'avaient dès lors pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique. La Cour a observé en particulier que l'enregistrement systématique des conversations dans un parloir à d'autres fins que la sécurité de la détention dénie à la fonction du parloir sa seule raison d'être, celle de maintenir une vie privée du détenu – relative – qui englobe l'intimité des propos tenus avec ses proches.

### **Kennedy c. Royaume-Uni**

18 mai 2010

Condamné pour homicide (dans une affaire controversée, certaines preuves ayant disparu et d'autres étant contradictoires) et libéré en 1996, le requérant a ensuite mené campagne contre les erreurs judiciaires. Soupçonnant la police d'intercepter ses communications concernant une petite entreprise qu'il venait de créer, il porta plainte auprès de la Commission des pouvoirs d'enquête (« la CPE »). Il fut finalement informé en 2005 que ses plaintes n'avaient donné lieu à aucune décision en sa faveur. Autrement dit, soit ses communications n'avaient pas été interceptées, soit la CPE tenait pour licite une interception éventuelle. La CPE ne lui donna aucun autre renseignement. Le requérant dénonçait l'interception alléguée de ses communications.

La Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que la législation du Royaume-Uni en matière d'interception de communications internes, combinée avec les précisions apportées par la publication d'un code de déontologie, décrivait avec une clarté suffisante les procédures concernant la délivrance et le fonctionnement des mandats d'interception ainsi que le traitement, la communication et la destruction des données recueillies. En outre, aucun élément n'indiquait qu'il y ait eu d'importantes lacunes dans l'application et la mise en œuvre du régime de surveillance. Dès lors, eu égard aux garanties contre une mauvaise utilisation des procédures ainsi qu'aux garanties plus générales offertes par le contrôle de la CPE, les mesures de surveillance litigieuses, pour autant qu'elles aient pu être appliquées au requérant, étaient justifiées sous l'angle de l'article 8 § 2 de la Convention.

### **Dragojević c. Croatie**

15 janvier 2015

Cette affaire concernait principalement la surveillance secrète des conversations d'une personne soupçonnée d'infractions à la législation sur les stupéfiants. Le requérant alléguait notamment que le juge d'instruction n'avait pas respecté la procédure prescrite par le droit interne pour apprécier effectivement si le recours à des mesures de surveillance secrète était nécessaire et justifié dans son cas particulier.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a estimé en particulier que la loi croate, telle qu'interprétée par les juridictions nationales, n'était pas assez claire quant au pouvoir discrétionnaire des autorités d'ordonner des mesures de surveillance et n'avait pas offert dans la pratique – dans le cas du requérant – des garanties suffisantes contre des abus éventuels.

Voir aussi : **Bašić c. Croatie**, arrêt du 25 octobre 2016 ; **Matanović c. Croatie**, arrêt du 4 avril 2017.

### R.E. c. Royaume-Uni (n° 62498/11)

27 octobre 2015

Le requérant, qui fut arrêté et détenu en Irlande du Nord à trois reprises dans le cadre du meurtre d'un policier, se plaignait en particulier du régime de surveillance secrète des consultations entre les détenus et leur avocat et entre les détenus vulnérables<sup>6</sup> et un « adulte approprié »<sup>7</sup>.

La Cour a examiné cette affaire du point de vue des principes dégagés par elle dans le domaine de l'interception des communications téléphoniques entre un avocat et son client, qui doit être entourée de garanties strictes. Elle a estimé que ces principes doivent s'appliquer à la surveillance secrète des consultations entre un avocat et son client au poste de police. En l'espèce, la Cour a conclu à la **violation de l'article 8** de la Convention en ce qui concerne la surveillance secrète des consultations juridiques. Elle a noté en particulier que des directives prévoyant des mesures pour le traitement, le stockage et la destruction sécurisés d'éléments obtenus au moyen d'une telle surveillance secrète étaient appliquées depuis le 2 juin 2010. Toutefois, au moment de la détention du requérant en mai 2010, ces directives n'étaient pas encore en vigueur. Dès lors, la Cour n'était pas convaincue que les dispositions législatives internes pertinentes en vigueur à l'époque des faits comportaient des garanties suffisantes pour la protection des consultations du requérant avec son avocat ayant fait l'objet d'une surveillance secrète. La Cour a par ailleurs conclu à la **non-violation de l'article 8** en ce qui concerne la surveillance secrète des consultations entre un détenu et un « adulte approprié ». Elle a à cet égard notamment estimé que ceux-ci ne sont pas protégés par le secret professionnel et qu'un détenu n'a donc pas les mêmes attentes quant au respect de leur caractère privé que pour une consultation juridique. En outre, la Cour était convaincue que les dispositions internes pertinentes, pour autant qu'elles concernaient la surveillance éventuelle des consultations entre un détenu et « l'adulte approprié », comportaient des garanties suffisantes contre les abus.

### Roman Zakharov c. Russie<sup>8</sup>

4 décembre 2015 (Grande Chambre)

Cette affaire concernait le système d'interception secrète des communications de téléphonie mobile en Russie. Le requérant, rédacteur en chef d'une maison d'édition, alléguait en particulier que les opérateurs de réseaux mobiles en Russie étaient tenus en vertu de la loi d'installer un dispositif permettant aux organes d'application des lois de mener à bien des mesures opérationnelles d'investigation et que, en l'absence de garanties suffisantes en droit russe, ce système rendait possible l'interception généralisée des communications.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que les dispositions du droit russe régissant l'interception de communications ne comportent pas de garanties adéquates et effectives contre l'arbitraire et le risque d'abus inhérent à tout système de surveillance secrète, risque qui est particulièrement élevé dans un système tel que celui de la Russie, où les services secrets et la police jouissent grâce à des moyens techniques d'un accès direct à l'ensemble des communications de téléphonie mobile. Plus particulièrement, la Cour a constaté des défaillances du cadre juridique dans les domaines suivants : les circonstances dans lesquelles les pouvoirs publics peuvent recourir à des mesures de surveillance secrète ; la durée de ces mesures, notamment les circonstances dans lesquelles elles doivent être levées ; les procédures relatives à l'autorisation de l'interception ainsi qu'à la conservation et à la destruction des données interceptées ; le contrôle des interceptions. De plus, l'effectivité des recours permettant de se plaindre de l'interception de communications est compromise par le fait qu'ils sont ouverts uniquement aux personnes qui sont à même de prouver l'interception, et par le

<sup>6</sup>. Un mineur ou une personne atteinte de troubles mentaux ou psychologiquement vulnérable.

<sup>7</sup>. Un « adulte approprié » peut être un proche ou un tuteur, ou encore une personne ayant une expérience des personnes atteintes de troubles mentaux ou psychologiquement vulnérables.

<sup>8</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.



fait que l'obtention d'une telle preuve est impossible en l'absence de tout système de notification ou de possibilité d'accès aux informations sur les interceptions.

Voir aussi, concernant des mesures de surveillance secrètes prises dans le cadre de procès pénaux : [Akhlyustin c. Russie](#), [Zubkov et autres c. Russie](#), [Moskalev c. Russie](#) et [Konstantin Moskalev c. Russie](#), arrêts du 7 novembre 2017<sup>9</sup>.

### **Szabó et Vissy c. Hongrie**

12 janvier 2016

Cette affaire concernait la législation hongroise, introduite en 2011, sur les opérations secrètes de surveillance antiterroriste. Les requérants se disaient notamment exposés au risque potentiel de faire l'objet de mesures injustifiées et exagérément intrusives dans le cadre juridique hongrois sur la surveillance secrète (à savoir l' « article 7/E (3) sur la surveillance »). Ils alléguaient en particulier que ce cadre légal incitait aux abus, faute notamment de contrôle juridictionnel.

La Cour a conclu en l'espèce à la **violation de l'article 8** de la Convention. Elle a admis que les formes prises par le terrorisme de nos jours avaient pour conséquence naturelle un recours par les gouvernements à des technologies de pointe, notamment à des techniques de surveillance massive des communications, afin d'éviter des incidents imminents. Cependant, elle a estimé que la législation en question ne fournissait pas les garanties nécessaires contre les abus. Notamment, pratiquement n'importe qui en Hongrie peut être soumis à une surveillance secrète, les nouvelles technologies permettant au gouvernement d'intercepter facilement des masses de données concernant des personnes se trouvant même en dehors de la catégorie initialement visée par l'opération. De plus, pareille mesure peut être ordonnée par le pouvoir exécutif sans aucun contrôle, sans faire l'objet d'une appréciation de la question de savoir si elle est strictement nécessaire et en l'absence de toute mesure de recours effectif, judiciaire ou autre. La Cour a par ailleurs conclu à la **non-violation de l'article 13** (droit à un recours effectif) de la Convention **combiné avec l'article 8**, rappelant que l'article 13 ne peut être interprété comme exigeant un recours contre l'état du droit interne.

### **Mustafa Sezgin Tanrikulu c. Turquie**

18 juillet 2017

Le requérant dénonçait une décision rendue par les juridictions nationales en 2005 qui avait autorisé pendant environ un mois et demi l'interception des communications électroniques de quiconque se trouvait en Turquie, notamment lui-même. Il alléguait en particulier que les mesures d'interception étaient contraires à la législation en vigueur à l'époque des faits. Il disait également avoir été privé d'un recours judiciaire effectif parce que les autorités nationales auraient refusé de mener une enquête sur ses allégations concernant l'interception de ses communications.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que dans la présente affaire le mandat d'interception n'était pas prévu par la loi. La Cour a également conclu à la **violation de l'article 13** (droit à un recours effectif) de la Convention.

### **Ben Faiza c. France**

8 février 2018

Voir ci-dessous, sous « Données GPS ».

### **Benedik c. Slovénie**

24 avril 2018

Cette affaire portait sur le fait que la police slovène ne s'était pas procuré de décision de justice aux fins de la consultation de données sur un abonné associées à une adresse IP dynamique que les autorités de police suisses avaient enregistrée lors de la surveillance des utilisateurs d'un réseau de partage de fichiers. L'accès à ces données permit

---

<sup>9</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

d'identifier le requérant, qui sur ce réseau avait partagé des fichiers, notamment des images pédopornographiques.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a jugé en particulier que l'utilisation par la police d'une certaine disposition juridique pour obtenir les données sur l'abonné associées à l'adresse IP dynamique n'avait pas satisfait à la norme de la Convention selon laquelle l'ingérence doit être « prévue par la loi ». La disposition en question manquait de clarté, n'offrait pratiquement aucune protection contre l'ingérence arbitraire, ne prévoyait pas de garanties contre l'abus ni de surveillance indépendante des pouvoirs de police en jeu.

### **Hambardzumyan c. Arménie**

5 décembre 2019

La requérante alléguait que les forces de l'ordre l'avaient placée sous surveillance secrète dans le cadre d'une enquête pénale sans disposer pour cela d'un mandat valide. Elle se plaignait en particulier des mesures de surveillance secrète prises à son égard et de l'utilisation des informations ainsi recueillies dans le cadre de la procédure dirigée contre elle.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la mesure de surveillance appliquée à la requérante n'avait pas fait l'objet d'un contrôle judiciaire adéquat et qu'elle n'était pas « prévue par la loi » au sens de la Convention. Elle a observé en particulier que le mandat n'avait pas été suffisamment précis quant à la personne qui faisait l'objet de la mesure de surveillance secrète. Or, pour la Cour, pareille imprécision est inacceptable lorsqu'il s'agit d'une mesure telle que la surveillance secrète, qui est de nature à porter gravement atteinte au droit au respect de la vie privée et familiale. Par ailleurs, le mandat n'indiquait pas les mesures spécifiques à mettre en œuvre à l'égard de la requérante. La Cour a en revanche conclu à la **non-violation de l'article 6** (droit à un procès équitable) de la Convention dans le cas de la requérante, jugeant que l'usage des données secrètement enregistrées n'avait pas été contraire aux exigences d'équité posées par l'article 6 § 1.

### **Privacy International et autres c. Royaume-Uni**

7 juillet 2020 (décision sur la recevabilité)

Les requérants – une ONG sise à Londres, un prestataire de services internet sis à Londres, une association de « hacktivistes » sise en Allemagne, deux sociétés sises aux États-Unis qui fournissent respectivement des services internet et des services de communication ainsi qu'un prestataire de services internet sis en Corée du Sud – croyaient que, pendant une période indéterminée, leurs systèmes avaient fait l'objet d'une ingérence, désignée familièrement par le terme « hacking », de la part du *Government Communications Headquarters* (GCHQ, service du renseignement électronique) et/ou du *Secret Intelligence Service* (MI6, service du renseignement extérieur) du Royaume-Uni. Ils soutenaient que le pouvoir conféré par l'article 7 de la loi de 1994 sur les services de renseignement<sup>10</sup> était dépourvu de base légale, que cet article ne posait aucune exigence d'autorisation judiciaire, qu'il n'y avait aucune information publique sur la manière dont il pouvait être utilisé pour autoriser une ingérence dans les systèmes, et qu'il n'y avait aucune obligation de filtrer les informations recueillies pour en exclure les données non pertinentes. Ils ajoutaient que la possibilité de saisir la Commission des pouvoirs d'enquête (*Investigatory Powers Tribunal*) ne constituait pas un recours effectif, cette commission ne statuant pas sur les cas relevant de l'article 7 de la loi en question.

La Cour a déclaré **irrecevables** les griefs des requérants tirés de l'article 8, de l'article 10 (liberté d'expression) et de l'article 13 (droit à un recours effectif) de la Convention, jugeant que, dans les circonstances de l'espèce, les requérants n'avaient pas donné aux juridictions nationales, notamment à la Commission des pouvoirs

<sup>10</sup>. L'article 7 de la loi de 1994 sur les services de renseignement (Intelligence Services Act 1994 – « l'ISA ») permet au ministre d'autoriser quelqu'un à réaliser hors des îles britanniques, sans encourir aucune sanction, un acte qui serait réprimé par la loi s'il était fait au Royaume-Uni.

d'enquête, l'occasion que l'article 35 (conditions de recevabilité) de la Convention a pour finalité de ménager en principe aux États contractants, à savoir celle d'examiner, c'est-à-dire de prévenir ou redresser la violation au regard de la Convention qui est alléguée contre cet État. La Cour a noté en particulier les arguments généraux avancés par les requérants, et soulignés aussi dans les interventions des tierces parties, selon lesquels la surveillance dénoncée était particulièrement intrusive et qu'il était nécessaire de prévoir des garanties dans ce domaine. À cet égard, elle a rappelé l'importance d'examiner le respect des principes de l'article 8 de la Convention lorsque les pouvoirs conférés à l'État sont obscurs, créant un risque d'arbitraire, surtout lorsque la technologie disponible est de plus en plus sophistiquée. Toutefois, cette importance renforce, dans le contexte de l'épuisement des voies de recours internes, la nécessité de donner aux tribunaux nationaux la possibilité de statuer sur ces questions lorsqu'ils en ont le potentiel.

### **Big Brother Watch et autres c. Royaume-Uni**

25 mai 2021 (Grande Chambre)

Ces requêtes ont été introduites après les révélations d'Edward Snowden (ancien agent contractuel de l'Agence nationale de sécurité américaine) sur l'existence de programmes de surveillance et de partage de renseignements entre les USA et le Royaume-Uni. Les requérantes, des journalistes et des organisations de défense des droits de l'homme, se plaignaient de trois régimes de surveillance mis en place au Royaume-Uni, à savoir 1) l'interception en masse de communications, 2) la réception d'éléments interceptés obtenus auprès de gouvernements et de services de renseignement étrangers et 3) l'obtention de données de communication auprès des fournisseurs de services de communication<sup>11</sup>.

La Grande Chambre a conclu : à l'unanimité, qu'il y avait eu **violation de l'article 8** de la Convention à raison du régime d'interception en masse ; à l'unanimité, qu'il y avait eu **violation de l'article 8** à raison du régime d'obtention de données de communication auprès des fournisseurs de services de communication ; par douze voix contre cinq, qu'il n'y avait **pas** eu **violation de l'article 8** à raison du régime britannique de demande d'éléments interceptés auprès de gouvernements et de services de renseignement étrangers ; à l'unanimité, qu'il y avait eu **violation de l'article 10** (liberté d'expression) de la Convention à raison tant du régime d'interception en masse que du régime d'obtention de données de communication auprès des fournisseurs de services de communication ; et, par douze voix contre cinq, qu'il n'y avait **pas** eu **violation de l'article 10** à raison du régime de demande d'éléments interceptés auprès de gouvernements et de services de renseignement étrangers. La Cour a considéré en particulier que, compte tenu des multiples menaces auxquelles les États doivent faire face dans les sociétés modernes, le recours à un régime d'interception en masse n'est pas en soi contraire à la Convention. Toutefois, elle a jugé que pareil régime doit être encadré par des « garanties de bout en bout », c'est-à-dire qu'au niveau national la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*. La Cour a par ailleurs estimé que le régime d'interception en masse en vigueur au Royaume-Uni à l'époque pertinente souffrait des lacunes suivantes : les interceptions en masse étaient autorisées par un ministre, et non par un organe indépendant de l'exécutif, les catégories de termes de recherche qui définissaient les types de communications susceptibles d'être examinées

---

<sup>11</sup>. À l'époque des faits, le régime d'interception en masse et d'obtention de données de communication auprès des fournisseurs de services de communication avait pour base légale la loi de 2000 portant réglementation des pouvoirs d'enquête (*Regulation of Investigatory Powers Act 2000*). Depuis lors, cette loi a été remplacée par la loi de 2016 sur les pouvoirs d'enquête (*Investigatory Powers Act 2016*). Les conclusions auxquelles la Grande Chambre est parvenue concernent uniquement les dispositions de la loi de 2000, qui formaient le cadre juridique en vigueur à l'époque des faits litigieux.

n'étaient pas mentionnées dans les demandes de mandat d'interception et les termes de recherche liés à un individu (c'est-à-dire les identifiants spécifiques tels que les adresses de courrier électronique) n'étaient pas soumis à une autorisation interne préalable. La Cour a également jugé que le régime d'interception en masse ne protégeait pas suffisamment les éléments journalistiques confidentiels. Elle a estimé par ailleurs que le dispositif d'obtention de données de communication auprès des fournisseurs de services de communication n'était pas prévu par la loi. En revanche, la Cour a considéré que les procédures autorisant le Royaume-Uni à demander des informations à des gouvernements et/ou à des services de renseignement étrangers présentaient des garanties suffisantes contre les abus et empêchaient les autorités britanniques d'utiliser ces demandes pour contourner leurs obligations découlant du droit interne et de la Convention.

### **Centrum För Rättvisa c. Suède**

25 mai 2021 (Grande Chambre)

Cette affaire portait sur le risque, allégué par la fondation requérante, que les communications que celle-ci entretient quotidiennement avec des particuliers, des organisations et des entreprises en Suède et à l'étranger par courrier électronique, par téléphone et par télécopie, souvent sur des sujets sensibles, aient pu ou puissent être interceptées et examinées dans le cadre d'activités de renseignement d'origine électromagnétique.

La Grande Chambre a conclu, par quinze voix contre deux, à la **violation de l'article 8** de la Convention. Elle a jugé, en particulier, que même si les caractéristiques principales du régime suédois d'interception en masse répondaient aux exigences de la Convention relatives à la qualité de la loi, le régime en question souffrait néanmoins de trois carences : l'absence de règle claire concernant la destruction des éléments interceptés qui ne contiennent pas de données à caractère personnel, le fait que ni la loi relative au renseignement d'origine électromagnétique ni aucun autre texte n'énonce l'obligation de prendre en compte les intérêts liés à la vie privée lorsqu'une décision de partage de renseignements avec des partenaires étrangers est adoptée, et l'absence de contrôle *a posteriori* effectif. Ces carences faisaient que le régime en cause ne satisfaisait pas à l'exigence de « garanties de bout en bout », qu'il excédait la marge d'appréciation accordée aux autorités de l'État défendeur à cet égard et, considéré dans son ensemble, n'offrait pas une protection adéquate et effective contre l'arbitraire et le risque d'abus.

Voir aussi, récemment :

### **Ringler c. Autriche**

12 mai 2020 (comité – décision sur la recevabilité)

### **Tretter et autres c. Autriche**

29 septembre 2020 (comité – décision sur la recevabilité)

### **Adomaitis c. Lituanie**

18 janvier 2022

### **Requêtes pendantes**

#### **Association confraternelle de la presse judiciaire c. France et 11 autres requêtes (n<sup>os</sup> 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 et 59621/15)**

Requêtes communiquées au gouvernement français le 26 avril 2017

Ces requêtes, qui ont été introduites par des avocats et des journalistes, ainsi que par des personnes morales en lien avec ces professions, concernent la loi française n° 2015-912 du 24 juillet 2015 relative au renseignement.

La Cour a communiqué les requêtes au gouvernement français et posé des questions aux parties sous l'angle des articles 8, 10 (liberté d'expression) et 13 (droit à un recours effectif) de la Convention.

*Requêtes similaires pendantes* : [Follorou c. France \(n° 30635/17\) et Johannes c. France \(n° 30636/17\)](#), communiquée au gouvernement français le 4 juillet 2017.

[Pietrzak c. Pologne \(n° 72038/17\) et Bychawska-Siniarska et autres c. Pologne \(n° 25237/18\)](#)

Requêtes communiquées au gouvernement polonais le 27 novembre 2019

Ces requêtes portent sur la législation polonaise autorisant un système de surveillance secrète des communications téléphoniques, postales et électroniques et celui de collecte des données relatives à ces communications (les « métadonnées »).

En novembre 2019, la Cour a [communiqué les requêtes au gouvernement polonais](#) et posé des questions aux parties sous l'angle des articles 8 (droit au respect de la vie privée et de la correspondance) et 13 (droit de recours effectif) de la Convention.

Onze tierces parties ont été autorisées à intervenir dans la procédure écrite, dont quatre ont été invitées à intervenir à l'audience de chambre qui s'est tenue au Palais des droits de l'homme le 27 septembre 2022.

[A.L. c. France \(n° 44715/20\) et E.J. c. France \(n° 47930/21\)](#)

Requêtes communiquées au gouvernement français le 8 décembre 2021

Ces requêtes portent en particulier sur l'infiltration par les autorités françaises du réseau de communication crypté « EncroChat » et sur la captation des données stockées et échangées avec les appareils connectés à ce réseau, leur copie et leur analyse.

La Cour a [communiqué les requêtes au gouvernement français](#) et posé des questions aux parties sous l'angle des articles 6 § 1 (droit à un procès équitable), 8 (droit au respect de la vie privée et de la correspondance), 13 (droit de recours effectif), 34 (droit de requête individuelle) et 35 (conditions de recevabilité) de la Convention.

## Surveillance de l'utilisation des ordinateurs par des employés

[Bărbulescu c. Roumanie](#)

5 septembre 2017 (Grande Chambre)

Cette affaire avait pour objet la décision d'une entreprise privée de mettre fin au contrat de travail d'un employé – le requérant – après avoir surveillé ses communications électroniques et avoir eu accès à leur contenu. Le requérant alléguait que la décision de son employeur reposait sur une violation de sa vie privée et que les juridictions nationales avaient failli à leur obligation de protéger son droit au respect de la vie privée et de la correspondance.

La Cour a conclu, par onze voix contre six, à la **violation de l'article 8** de la Convention, jugeant que les autorités roumaines n'avaient pas correctement protégé le droit du requérant au respect de sa vie privée et de sa correspondance. Elles n'avaient donc pas ménagé un juste équilibre entre les intérêts en jeu. En particulier, les juridictions nationales n'avaient pas, d'une part, vérifié si le requérant avait été préalablement averti par son employeur de la possibilité que ses communications soient surveillées et n'avaient pas non plus, d'autre part, tenu compte du fait qu'il n'avait été informé ni de la nature ni de l'étendue de cette surveillance, ni du degré d'intrusion dans sa vie privée et sa correspondance. De surcroît, les juridictions nationales n'avaient pas déterminé, premièrement, quelles raisons spécifiques avaient justifié la mise en place des mesures de surveillance, deuxièmement, si l'employeur aurait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance du requérant et, troisièmement, si l'accès au contenu des communications avait été possible à son insu.

[Libert c. France](#)

22 février 2018

Cette affaire concernait le licenciement d'un employé de la SNCF après que la saisie de son ordinateur professionnel avait révélé le stockage de fichiers à caractère pornographique et de fausses attestations réalisées au bénéfice de tiers. Le requérant se plaignait en particulier du fait que son employeur avait ouvert des fichiers personnels figurant sur le disque dur de son ordinateur professionnel en dehors de sa présence.

La Cour a conclu à l'**absence de violation de l'article 8** de la Convention, jugeant que les autorités françaises n'avaient pas excédé la marge d'appréciation dont elles disposaient en l'espèce. Elle a constaté en particulier que la consultation des fichiers par l'employeur du requérant répondait à un but légitime de protection des droits de l'employeur, qui peut légitimement vouloir s'assurer que ses salariés utilisent les équipements informatiques qu'il met à leur disposition en conformité avec leurs obligations contractuelles et la réglementation applicable. La Cour a également observé que le droit français contenait un principe visant à la protection de la vie privée suivant lequel, si l'employeur pouvait ouvrir les fichiers professionnels, il ne pouvait subrepticement ouvrir les fichiers identifiés comme étant personnels. Il ne pouvait procéder à leur ouverture qu'en présence de l'employé. Les juridictions internes avaient jugé que ce principe ne faisait pas obstacle à ce que l'employeur ouvre les fichiers litigieux, ceux-ci n'ayant pas été dûment identifiés comme étant privés. Enfin, la Cour a considéré que les juridictions internes avaient correctement examiné le moyen du requérant tiré d'une violation de son droit au respect de sa vie privée et estimé que la décision de ces juridictions s'était fondée sur des motifs pertinents et suffisants.

## Surveillance vidéo

### Peck c. Royaume-Uni

29 janvier 2003

Voir ci-dessous, sous « Divulgence de données personnelles ».

### Köpke c. Allemagne

5 octobre 2010 (décision sur la recevabilité)

La requérante, qui travaillait comme caissière dans un supermarché, fut licenciée sans préavis pour vol, à la suite d'une mesure de surveillance vidéo secrète mise en œuvre par son employeur avec l'aide d'une agence de détectives privés. Elle contesta en vain son licenciement devant les juridictions du travail. De même, son recours constitutionnel fut rejeté.

La Cour a déclaré **irrecevable** (manifestement mal fondé) le grief de la requérante tiré de l'article 8 de la Convention. Elle a conclu que les autorités internes avaient ménagé un juste équilibre entre le droit au respect de la vie privée de l'employée, l'intérêt pour son employeur de protéger son droit au respect de ses biens et l'intérêt public d'une bonne administration de la justice. La Cour a observé cependant que le poids respectif des différents intérêts concurrents en jeu pourrait évoluer à l'avenir, compte tenu de la mesure dans laquelle de nouvelles technologies de plus en plus sophistiquées rendent possibles les atteintes à la vie privée.

### Antović et Mirković c. Monténégro

28 novembre 2017

Dans cette affaire, deux professeurs de l'École de mathématiques de l'Université du Monténégro soulevaient un grief tiré d'une atteinte alléguée à la vie privée, qui aurait résulté de l'installation d'un système de vidéosurveillance dans leurs lieux d'enseignement. Ils soutenaient qu'il n'y avait eu aucun contrôle effectif sur les informations collectées et que la surveillance était illégale. Les tribunaux internes rejetèrent toutefois leur action en réparation, considérant qu'aucune question de vie privée ne se posait, car les amphithéâtres où les intéressés enseignaient étaient des lieux publics.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la vidéosurveillance en cause n'était pas prévue par la loi. Elle a tout d'abord rejeté l'exception d'irrecevabilité soulevée par le Gouvernement lequel arguait qu'aucune question relative à la vie privée ne se posait parce que la zone sous surveillance était un lieu public de travail. À cet égard, la Cour a relevé en particulier qu'elle avait considéré auparavant que la vie privée pouvait inclure les activités professionnelles. Elle a estimé que c'était le cas dans la situation des requérants et que l'article 8 était donc applicable. Sur le fond, la Cour a ensuite jugé que la vidéosurveillance constituait une ingérence

dans l'exercice par les requérants de leur droit à la vie privée et que les éléments de preuve montraient que cette vidéosurveillance méconnaissait les dispositions du droit interne. En effet, les tribunaux internes n'avaient même pas cherché à trouver une justification légale pour la surveillance, car ils avaient décidé dès le départ qu'il n'y avait aucune atteinte à la vie privée.

### **López Ribalda et autres c. Espagne**

17 octobre 2019 (Grande Chambre)

Cette affaire concernait la mise sous vidéosurveillance secrète d'employées, à l'origine de leur licenciement. Celles-ci estimaient inéquitable le recours à une vidéosurveillance dissimulée et l'utilisation par les juridictions nationales des données ainsi obtenues aux fins de conclure à la légitimité de leurs licenciements. Les requérantes qui avaient signé des accords transactionnels allèguent également que la signature des accords avait été obtenue sous la contrainte, après le visionnage des enregistrements vidéo, et que ces accords n'auraient pas dû être admis comme preuves de la validité de leurs licenciements.

La Grande Chambre a conclu à la **non-violation de l'article 8** de la Convention dans le chef des cinq requérantes. Elle a jugé en particulier que les tribunaux espagnols avaient minutieusement mis en balance les droits des requérantes – des employées d'un supermarché soupçonnées de vols – et ceux de l'employeur, et qu'ils avaient examiné en détail la justification de la vidéosurveillance. Un des arguments des requérantes était qu'elles n'avaient pas été averties au préalable de leur mise sous surveillance, malgré une obligation légale, mais la Cour a jugé qu'une telle mesure était clairement justifiée en raison des soupçons légitimes d'irrégularités graves et des pertes constatées, considérant l'étendue et les conséquences de cette mesure. En l'espèce, les tribunaux internes avaient donc conclu, sans outrepasser leur marge d'appréciation, que cette surveillance avait été proportionnée et légitime. La Cour a conclu également dans cette affaire à la **non-violation de l'article 6 § 1** (droit à un procès équitable) de la Convention, jugeant en particulier que l'utilisation comme preuves des images obtenues par vidéosurveillance n'avait pas porté atteinte au caractère équitable de la procédure.

## Conservation et exploitation de données personnelles

« La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (...). La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment assurer que ces données soient pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (...). [Il] doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (...). » (*S. et Marper c. Royaume-Uni*, arrêt (Grande Chambre) du 4 décembre 2008, § 103)

## Dans le contexte de la justice pénale

### **Perry c. Royaume-Uni**

17 juillet 2003

Le requérant fut arrêté après qu'eut été commise une série de vols à main armée sur la personne de chauffeurs de taxi, puis relâché en attendant que se tienne une séance d'identification. Comme il ne s'était pas présenté à la séance prévue ni à plusieurs autres

séances ultérieures, la police sollicita l'autorisation de le filmer en secret avec une caméra vidéo. Le requérant se plaignait que la police l'avait filmé en secret en vue de l'identifier puis avait utilisé le film vidéo dans le cadre des poursuites dirigées contre lui.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a relevé que rien n'indiquait que le requérant s'attendait à ce qu'on le filme au poste de police à des fins d'identification au moyen d'un enregistrement vidéo ni à ce que le film soit éventuellement utilisé comme preuve à charge lors de son procès. Le stratagème adopté par la police avait outrepassé l'utilisation normale de ce type de caméra et constitué une ingérence dans l'exercice par le requérant de son droit au respect de sa vie privée. Cette ingérence n'était par ailleurs pas prévue par la loi, la police n'ayant pas respecté les procédures énoncées par le code applicable : elle n'avait pas obtenu le consentement du requérant, ne l'avait pas averti de l'enregistrement vidéo et, de surcroît, ne l'avait pas informé de ses droits à cet égard.

### **S. et Marper c. Royaume-Uni**

4 décembre 2008 (Grande Chambre)

Cette affaire concernait la rétention indéfinie dans une base de donnée des empreintes digitales et données ADN (échantillons cellulaires et profil ADN<sup>12</sup>) des requérants après que les procédures pénales dirigées contre eux se furent soldées par un acquittement pour l'un et un classement sans suite pour l'autre.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la conservation en cause s'analysait en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne pouvait passer pour nécessaire dans une société démocratique. La Cour a considéré en particulier que l'usage des techniques scientifiques modernes dans le système de la justice pénale ne pouvait être autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part, et que tout État revendiquant un rôle de pionnier dans l'évolution de nouvelles technologies portait la responsabilité particulière de « trouver le juste équilibre » en la matière. Elle a conclu que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il avait été appliqué aux requérants en l'espèce, ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents en jeu.

### **B.B. c. France (n° 5335/06), Gardel c. France et M.B. c. France (n° 22115/06)**

17 décembre 2009

Les requérants dans ces affaires, qui avaient été condamnés à des peines de réclusion criminelle de viol sur mineurs de 15 ans par personne ayant autorité, se plaignaient en particulier de leur inscription au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (« FIJAIS »).

Dans les trois affaires, la Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que l'inscription au FIJAIS, telle qu'elle avait été appliquée aux requérants, avait ménagé un juste équilibre entre les intérêts privés et publics concurrents en jeu. La Cour a réaffirmé en l'espèce que la protection des données à caractère personnel joue un rôle fondamental dans le respect de la vie privée et familiale, d'autant plus quand il s'agit de données personnelles soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Cela étant, la Cour ne saurait mettre en doute les objectifs de prévention du fichier en question. En outre, les requérants ayant la possibilité concrète de présenter une requête en effacement des données, la Cour a estimé que la durée de conservation des données – de 30 maximum – n'était pas disproportionnée au regard du but poursuivi par la mémorisation des informations. Enfin, la consultation de telles données par les autorités

---

<sup>12</sup>. Les profils ADN sont des données numériques qui sont stockées sur support électronique dans la base de données ADN du Royaume-Uni avec des renseignements sur la personne à laquelle ces données se rapportent.



judiciaires, de police et administratives était régie par une obligation de confidentialité et des circonstances précisément déterminées.

Voir aussi : [J.P.D. c. France \(n° 55432/10\)](#), décision (irrecevable) du 16 septembre 2014.

### [Uzun c. Allemagne](#)

2 septembre 2010

Voir ci-dessus, sous « Collecte de données personnelles », « Données GPS ».

### [Dimitrov-Kazakov c. Bulgarie](#)

10 février 2011

Le requérant fut inscrit comme « délinquant » dans les registres de la police, après avoir été interrogé au sujet d'un viol – aucun acte d'accusation n'ayant été établi par la suite. Il fit ensuite l'objet de plusieurs contrôles de police en relation avec des plaintes pour viol ou avec des disparitions de jeunes filles. L'intéressé se plaignait de cette inscription au registre de la police et de n'avoir disposé d'aucun recours pour s'en plaindre.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que l'inscription au registre de la police n'était pas « prévue par la loi » au sens de cet article. Elle a en outre conclu à la **violation de l'article 13** (droit à un recours effectif) de la Convention combiné avec l'article 8, en raison de l'absence de recours effectif à cet égard.

### [Shimovolos c. Russie](#)<sup>13</sup>

21 juin 2011

Cette affaire concernait l'enregistrement d'un militant des droits de l'homme dans une base de données relative aux surveillances secrètes et le suivi de ses déplacements, ainsi que son arrestation survenue dans ce contexte.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a notamment relevé que la création et la mise à jour de la base de données en cause ainsi que ses modalités de fonctionnement étaient régies par un arrêté ministériel qui n'avait jamais été publié ni d'une autre manière été rendu accessible au public. En conséquence, la Cour a estimé que le droit interne n'indiquait pas avec une clarté suffisante la portée et le mode d'exercice du pouvoir discrétionnaire conféré aux autorités internes pour recueillir et conserver dans la base de données des informations sur la vie privée de particuliers. Singulièrement, le droit interne ne présentait, sous une forme accessible au public, aucune indication des garanties minimales contre les abus.

### [Khelili c. Suisse](#)

18 octobre 2011

Lors d'un contrôle en 1993, la police du canton de Genève trouva sur la requérante des cartes de visite sur lesquelles on pouvait lire « Gentille, jolie femme fin trentaine attend ami pour prendre un verre de temps en temps ou sortir. Tel. (...) ». La requérante alléguait que, suite à cette découverte, la police l'aurait fichée comme prostituée, profession qu'elle a toujours contesté exercer. Elle soutenait que la mémorisation de données prétendument erronées relatives à sa vie privée aurait violé son droit au respect de sa vie privée.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la mémorisation, dans le dossier de police, d'une donnée à caractère personnel, prétendument erronée, avait violé le respect de la vie privée de la requérante et que le maintien de la mention « prostituée » pendant des années n'avait été ni justifié, ni nécessaire dans une société démocratique. La Cour a notamment observé que la mention litigieuse pouvait nuire à la réputation de la requérante et, comme elle le prétendait, rendre plus difficile sa vie quotidienne, étant donné que les informations figurant dans les dossiers de police pouvaient être transmises aux autorités. Cela était d'autant plus important de nos jours que des données à caractère personnel sont soumises à un traitement automatique qui facilite considérablement l'accès à celles-ci et

<sup>13</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

leur diffusion. La requérante avait donc un intérêt considérable à voir la mention « prostituée » biffée des fichiers et dossiers de police.

### **M.M. c. Royaume-Uni (n° 24029/07)**

13 novembre 2012

En 2000, la requérante fut arrêtée par la police après avoir disparu pendant une journée avec son petit-fils, un nourrisson, car elle voulait empêcher le départ de celui-ci pour l'Australie à la suite de l'échec du mariage de son fils. Les autorités décidèrent de ne pas la poursuivre, mais elle reçut un avertissement pour enlèvement d'enfant. Cet avertissement devait à l'origine demeurer sur son casier judiciaire pendant cinq ans mais, à la suite d'un changement de politique concernant les affaires dans lesquelles la partie lésée était un enfant, cette période fut prolongée à vie. La requérante se plaignait de la conservation et de la possibilité de divulguer des données concernant son avertissement pendant une durée illimitée ainsi que de l'impact de ces mesures sur ses perspectives d'emploi.

La Cour a conclu à la **violation de l'article 8** de la Convention. Eu égard à l'effet cumulé des défauts constatés, la Cour n'était en effet pas convaincue que le système de conservation et de divulgation des données relatives aux antécédents judiciaires présentait des garanties suffisantes permettant d'éviter que les données relatives à la vie privée de la requérante soient divulguées, en violation de ses droits au respect de sa vie privée, et elle a dès lors jugé que l'on ne saurait considérer que la conservation et la divulgation des données relatives à l'avertissement infligé à la requérante étaient prévues par la loi au sens de l'article 8. La Cour a observé en particulier que, bien que les données figurant dans le casier judiciaire soient, dans un certain sens, des informations publiques, leur mémorisation systématique dans les fichiers centraux signifie qu'elles peuvent être divulguées bien après l'événement, lorsque tout le monde, hormis la personne concernée, aura vraisemblablement oublié l'incident, en particulier lorsque, comme en l'espèce, l'avertissement a été donné en privé. Par conséquent, au fil du temps, la condamnation ou l'avertissement deviennent partie intégrante de la vie privée d'une personne, qui doit être respectée.

### **M.K. c. France (n° 19522/09)**

18 avril 2013

En 2004 et 2005, le requérant fit l'objet de deux enquêtes pour vol de livres. Il fut relaxé à l'issue de la première procédure. La seconde fut classée sans suite. En ces deux occasions, ses empreintes furent relevées et enregistrées au fichier automatisé des empreintes digitales. En 2006, l'intéressé demanda l'effacement de ses empreintes du fichier en question. Il fut fait droit à sa demande mais uniquement concernant les prélèvements effectués lors de la première procédure. Le requérant se plaignait du fait que la conservation des données le concernant au fichier automatisé des empreintes digitales portait atteinte au respect de sa vie privée.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la conservation litigieuse s'analysait en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne pouvait passer pour nécessaire dans une société démocratique. La Cour a observé en particulier que l'État français avait outrepassé sa marge d'appréciation en la matière, le régime de conservation dans le fichier litigieux des empreintes digitales de personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il avait été appliqué au requérant en l'espèce, ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu.

### **Peruzzo et Martens c. Allemagne**

4 juin 2013 (décision sur la recevabilité)

Les requérants, qui avaient été condamnés pour des infractions pénales graves, se plaignaient des décisions prises par les juridictions nationales, en vertu desquelles ils devaient subir un prélèvement de matériel cellulaire et les informations seraient conservées dans une base de données sous la forme de profils ADN aux fins de faciliter les enquêtes à venir sur d'éventuelles infractions.

La Cour a déclaré la requête **irrecevable** pour défaut manifeste de fondement. Elle a jugé que les dispositions du droit allemand applicables à la collecte et la conservation des échantillons d'ADN prélevés sur les personnes reconnues coupables d'infractions présentant – comme en l'espèce – une certaine gravité avaient ménagé un juste équilibre entre les intérêts privés et les intérêts publics concurrents en cause dans la présente affaire et qu'elles relevaient de la marge d'appréciation acceptable de l'État défendeur.

Voir aussi : **W. c. Pays-Bas (n° 20689/08)**, décision (irrecevable) du 20 janvier 2009.

### **Brunet c. France**

18 septembre 2014

Le requérant se plaignait notamment de l'atteinte à sa vie privée découlant de son inscription dans le fichier STIC (« Système de traitement des infractions constatées ») – un fichier de police répertoriant les informations provenant des comptes rendus d'enquêtes et recensant notamment les personnes mises en cause et les victimes – malgré le classement sans suite de la procédure pénale engagée contre lui.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que l'État français avait outrepassé sa marge d'appréciation en la matière, que la conservation litigieuse s'analysait en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne pouvait passer pour nécessaire dans une société démocratique. La Cour a considéré en particulier que le requérant n'avait pas disposé d'une possibilité réelle de demander l'effacement du STIC des informations le concernant et que la durée de conservation de ces données, qui était de vingt ans, était en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum.

### **Karabeyoğlu c. Turquie**

7 juin 2016

Cette affaire concernait une mesure de surveillance téléphonique dont avait fait l'objet le requérant, procureur, dans le cadre d'une enquête pénale relative à une organisation illégale dénommée *Ergenekon*, et l'utilisation des données recueillies dans le cadre d'une autre enquête, disciplinaire en l'espèce.

La Cour a conclu à la **non-violation de l'article 8** de la Convention concernant les écoutes téléphoniques relatives à l'enquête pénale et à la **violation de l'article 8** concernant l'utilisation, dans le cadre de l'enquête disciplinaire, des renseignements obtenus par le biais des écoutes téléphoniques. La Cour a jugé en particulier que, dans le cadre de l'enquête pénale, le requérant avait joui du degré minimal de protection requis par la prééminence du droit dans une société démocratique, le placement sur écoutes téléphoniques ayant été décidé en raison de l'existence de soupçons objectivement raisonnables et la mise en œuvre de la mesure ayant été conforme à la législation. Pour la Cour, l'ingérence dans le droit du requérant au respect de sa vie privée avait été nécessaire à la protection de la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales. La Cour a cependant jugé que l'utilisation de ces données dans le cadre d'une enquête disciplinaire n'était pas prévue par la loi et a estimé que cette situation avait constitué un double non-respect de la législation, à savoir l'utilisation des données en dehors du but pour lequel elles avaient été collectées et leur non-destruction dans le délai de 15 jours après la fin de l'enquête pénale. La Cour a également conclu dans cette affaire à la **violation de l'article 13** (droit à un recours effectif) de la Convention, constatant que, dans le cadre des enquêtes pénale et disciplinaire, le requérant n'avait pas eu à sa disposition une voie de recours interne lui permettant de faire examiner la compatibilité de l'ingérence avec son droit au respect de sa vie privée et de sa correspondance.

### **Figueiredo Teixeira c. Andorre**

8 novembre 2016

Cette affaire concernait la conservation et la communication à l'autorité judiciaire des données des appels téléphoniques du requérant suspecté de délit majeur de trafic de stupéfiants. L'intéressé soutenait en particulier que le stockage des données relatives à

ses communications téléphoniques avait constitué une ingérence injustifiée dans son droit à la vie privée.

La Cour a conclu à la **non-violation de l'article 8** de la Convention. Elle a jugé en particulier que l'ingérence litigieuse étant prévue en droit andorran par l'article 87 du code de procédure pénale et par la loi qualifiée n° 15/2003 relative à la protection des données personnelles, le détenteur d'une carte prépayée de téléphonie mobile pouvait raisonnablement attendre à se voir appliquer ces normes. La Cour a par ailleurs observé que la procédure andorrane offrait de nombreuses garanties contre les comportements arbitraires dès lors que c'est un juge (*batlle*) qui apprécie la nécessité de la mesure de transmission des données ainsi que sa proportionnalité eu égard aux indices obtenus et à la gravité du délit sous-jacent. La Cour a dès lors conclu que, en l'espèce, l'équilibre entre le droit à la vie privée du requérant et la prévention des infractions pénales avait été respecté.

### **Dagregorio et Mosconi c. France**

30 mai 2017 (décision sur la recevabilité)

Les requérants sont deux syndicalistes ayant participé à l'occupation et au blocage du navire de ligne « Pascal Paoli » de la Société nationale Corse Méditerranée (SNCM) lors de l'opération de reprise de la société par un opérateur financier. L'affaire concernait leur refus de se soumettre à un prélèvement biologique destiné à un enregistrement dans le fichier national automatisé des empreintes génétiques (FNAEG). Condamnés en première instance et en appel, les requérants ne formèrent pas de pourvoi en cassation.

La Cour a déclaré la requête **irrecevable** pour non-épuisement des voies de recours internes. Elle a souligné en particulier qu'en l'absence de précédent jurisprudentiel applicable à la situation des requérants, un doute existait quant à l'efficacité d'un pourvoi en cassation en raison d'une décision rendue par le Conseil constitutionnel. La Cour a considéré que c'est donc un point qui devait être soumis à la Cour de cassation. Le simple fait de nourrir des doutes quant aux perspectives de succès d'un recours donné ne constituait pas une raison propre à justifier la non-utilisation du recours en question.

### **Aycaquer c. France**

22 juin 2017

Le requérant dénonçait une atteinte à son droit au respect de sa vie privée, en raison de l'ordre qui lui avait été fait de se soumettre à un prélèvement biologique destiné à un enregistrement dans le fichier national automatisé des empreintes génétiques (FNAEG) et pour lequel son refus d'obtempérer avait donné lieu à une condamnation pénale.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a observé en particulier que le Conseil constitutionnel avait rendu, le 16 septembre 2010, une décision déclarant que les dispositions relatives au FNAEG étaient conformes à la Constitution, sous réserve entre autres « de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées ». La Cour a noté qu'à ce jour cette réserve n'avait pas reçu de suite appropriée et qu'aucune différenciation n'était actuellement prévue en fonction de la nature et de la gravité des infractions commises. La Cour a par ailleurs estimé que le régime de conservation des profils ADN dans le FNAEG n'offrait pas, en raison de sa durée et de l'absence de possibilité d'effacement, de protection suffisante aux intéressés. Cette circonstance ne traduisait donc pas de juste équilibre entre les intérêts publics et privés en jeu.

### **Catt c. Royaume-Uni**

24 janvier 2019

Le requérant, un militant de longue date, se plaignait de la collecte et de la conservation, dans une base de données de la police relative à l'« extrémisme national », de données personnelles le concernant.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a jugé en particulier que les informations détenues sur le requérant révélaient ses opinions politiques et

qu'elles nécessitaient de ce fait une protection particulière. Elle a tenu compte également de l'âge du requérant, qui avait 94 ans, et du fait qu'il ne s'était jamais rendu coupable d'actes de violence et qu'il était peu probable qu'il en commette à l'avenir. La Cour a également observé que si la collecte d'informations sur son compte avait été justifiée, leur conservation ne l'avait pas été, compte tenu notamment de l'absence de garanties telles que des délais.

### **Gaughran c. Royaume-Uni**

13 février 2020

Cette affaire concernait la conservation sans limitation de durée des données personnelles (profil ADN, empreintes digitales et photographie) d'un homme qui avait été reconnu coupable de conduite en état d'ivresse en Irlande du Nord et dont la condamnation avait été rayée de son casier judiciaire à l'expiration du délai prévu par la loi.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que le Royaume-Uni avait outrepassé la marge d'appréciation qui était la sienne, et que la conservation litigieuse s'analysait en une atteinte disproportionnée au droit du requérant au respect de sa vie privée, ne pouvant passer pour nécessaire dans une société démocratique. La Cour a précisé en particulier que ce n'est pas la durée de la détention des données en question qui avait été déterminante, mais l'absence de certaines garanties. Dans le cas du requérant, les autorités avaient décidé de conserver sans limitation de durée les données personnelles le concernant, sans tenir compte ni de la gravité de l'infraction commise ni de la nécessité de conserver les données en question sans limitation de durée, et sans lui offrir une réelle possibilité de réexamen. Notant également que la technologie utilisée de nos jours est plus complexe que les juridictions internes ne l'avaient envisagé dans cette affaire, notamment en ce qui concerne la conservation et l'analyse des photographies, la Cour a considéré que la conservation des données personnelles du requérant ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents.

### **Algirdas Butkevičius c. Lituanie**

14 juin 2022

Cette affaire portait sur une conversation téléphonique entre le requérant – qui était à l'époque le Premier ministre de la Lituanie – et un maire qui avait été secrètement enregistrée au cours d'une enquête préliminaire sur d'éventuels faits de corruption dans le domaine de l'aménagement du territoire puis rendue publique lors d'une audition de la Commission anti-corruption du Parlement lituanien (*Seimas*). Le requérant alléguait que, en divulguant la conversation téléphonique aux médias, les autorités de l'État avaient violé son droit à la vie privée et à la correspondance, soutenant en particulier que le procureur et la Commission anticorruption n'avaient pas adéquatement protégé ces informations comme la loi les y obligeait.

La Cour a conclu à la **non-violation de l'article 8** (droit au respect de la vie privée et de la correspondance) de la Convention dans le chef du requérant, jugeant que, quand bien même la réputation de l'intéressé auprès de ses collègues eût été atteinte par la divulgation de sa conversation téléphonique, aucun élément de fait, et surtout aucun élément de preuve, n'indiquait qu'elle avait été affectée de manière disproportionnée. La Cour a relevé en particulier que le requérant n'avait évoqué aucune répercussion concrète et tangible que la divulgation par les médias de la conversation téléphonique aurait eue sur sa vie privée, d'autant qu'il n'avait pas été reconnu coupable et que la Commission supérieure d'éthique n'avait rien relevé de problématique dans la conversation. Elle a également rappelé dans la présente affaire l'importance que revêt le contrôle du public dans les cas éventuels de corruption politique.

### **Haščák c. Slovaquie**

23 juin 2022

Cette affaire portait sur une opération de surveillance (« l'opération Gorilla ») menée en 2005 et 2006 par le service de renseignements slovaque (« le SIS ») et les informations

obtenues par ce moyen. Le requérant – un homme d'affaires de premier plan, membre d'une société financière influente et l'un des associés du requérant dans l'affaire [Zoltán Varga c. Slovaquie](#) (arrêt du 20 juillet 2021) – alléguait en particulier que la mise en œuvre de deux mandats de surveillance délivrés au milieu des années 2000 par le tribunal régional de Bratislava n'avait pas fait l'objet d'une supervision et d'un contrôle effectifs, que le cadre applicable n'offrait aucune protection aux victimes collatérales des mesures de surveillance et que les règles internes applicables à la conservation d'éléments relevant du renseignement étaient inadéquates.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention concernant la mise en œuvre des deux mandats litigieux et la conservation des documents analytiques. Elle a tout d'abord constaté que les griefs formulés par le requérant sur le terrain de l'article 8 étaient dans une large mesure similaires à ceux examinés dans l'affaire [Zoltán Varga](#) et qu'ils s'inscrivaient dans un contexte factuel et juridique analogue. En conséquence, elle a décidé d'appliquer cette jurisprudence à la présente affaire. La Cour a observé en particulier que si l'opération litigieuse avait une base légale, elle n'en présentait pas moins de nombreuses insuffisances, dont certaines avaient été constatées au niveau interne à l'occasion des plaintes formulées par M. Varga et des actions exercées par lui. Bien que les juridictions internes n'aient pas procédé aux mêmes constatations dans l'affaire du requérant, celles-ci demeuraient pertinentes aux fins de l'examen de son cas. Comme elle l'a fait dans l'affaire [Zoltán Varga](#), la Cour a jugé que pour mettre en œuvre les mandats de surveillance litigieux, le SIS avait joui dans les faits d'un pouvoir discrétionnaire illimité qui ne s'était accompagné d'aucune mesure de protection contre les ingérences arbitraires, comme l'exigeait pourtant le principe de la prééminence du droit. Cette situation était aggravée par le fait incontesté que le requérant n'était pas personnellement visé par la surveillance ordonnée par le premier des deux mandats, qu'il avait affirmé sans être contredit que la loi ne protégeait pas les victimes collatérales des mesures de surveillance et que le statut juridique et pratique de l'enregistrement audio découvert en 2018 et vraisemblablement réalisé par le SIS était totalement incertain. Enfin, la Cour a relevé qu'elle avait déjà constaté, dans l'affaire [Zoltán Varga](#), que la conservation des documents analytiques obtenus dans le cadre de l'opération de surveillance litigieuse avait été soumise à des règles confidentielles appliquées en l'absence de tout contrôle extérieur, et elle avait en conséquence conclu que cette conservation n'était pas prévue par la loi. Elle a estimé que ces conclusions s'appliquaient aussi à la présente affaire.

*Voir aussi*, parmi d'autres :

**[Caruana c. Malte](#)**

15 mai 2018 (décision sur la recevabilité)

**[P.N. c. Allemagne \(n° 74440/17\)](#)**

11 juin 2020

## Dans le contexte de la santé

**[Chave née Jullien c. France](#)**

9 juillet 1991 (décision de la Commission européenne des droits de l'homme<sup>14</sup>)

Cette affaire concernait la mémorisation dans le dossier d'un hôpital psychiatrique de données relatives à l'internement d'office de la requérante dont l'illégalité avait été reconnue par les tribunaux français. L'intéressée estimait en particulier que le maintien sur un fichier d'indications concernant son internement constituait une ingérence dans sa vie privée et souhaitait que les mentions en question disparaissent de ce type de fichier.

---

<sup>14</sup>. La Commission européenne des droits de l'homme, qui a siégé à Strasbourg de juillet 1954 à octobre 1999, est un organe qui, ensemble avec la Cour européenne des droits de l'homme et le Comité des Ministres du Conseil de l'Europe, contrôlait le respect par les États contractants des obligations assumées par eux en vertu de la Convention européenne des droits de l'homme. La Commission a disparu lorsque la Cour est devenue permanente le 1<sup>er</sup> novembre 1998.

La Commission a déclaré la requête **irrecevable** pour défaut manifeste de fondement. Elle a observé en particulier que la consignation des informations concernant les malades mentaux répondait au but légitime que représente le bon fonctionnement du service public hospitalier, mais aussi à celui de protéger les droits des malades eux-mêmes, spécialement en cas d'internement d'office. En l'espèce, la Commission a relevé notamment que les informations litigieuses étaient protégées par des règles de confidentialité appropriées. En outre, ces documents ne pouvaient être assimilés à des fichiers et n'étaient en aucune manière accessibles au public mais seulement à des catégories limitativement énumérées de personnes extérieures à l'établissement. Dès lors, la Commission a jugé que l'ingérence subie par la requérante n'avait pas été disproportionnée au but légitime poursuivi, à savoir la protection de la santé.

### **L.L. c. France (n° 7508/02)**

10 octobre 2006

Le requérant dénonçait notamment la production et l'utilisation en justice, dans le cadre d'une procédure de divorce, de pièces médicales le concernant, sans son consentement et sans qu'un médecin expert n'eût été commis à cet effet.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que l'ingérence subie par le requérant dans sa vie privée n'avait pas été justifiée au vu du rôle fondamental joué par la protection des données à caractère personnel. Elle a notamment observé que ce n'est qu'à titre subsidiaire que les juridictions françaises avaient invoqué la pièce médicale litigieuse pour fonder leurs décisions, et il apparaissait donc qu'elles auraient pu l'écartier tout en parvenant à la même conclusion. La Cour a en outre relevé que la législation française n'assortissait pas de garanties suffisantes l'utilisation de données relevant de la vie privée des parties dans ce type de procédure, ce qui justifiait à plus forte raison un strict contrôle de la nécessité de telles mesures.

### **Drelon c. France**

8 septembre 2022<sup>15</sup>

Voir ci-dessus, sous « Collecte de données personnelles », « Données reflétant l'orientation sexuelle ».

Voir aussi, récemment :

### **Mockuté c. Lituanie**

27 février 2018

## Données fiscales

### **Requêtes pendantes**

#### **L.B. c. Hongrie (n° 36345/16)**

12 janvier 2021 (arrêt de chambre) – affaire renvoyée devant la Grande Chambre en mai 2021

Cette affaire concerne la publication par l'administration fiscale des données personnelles du requérant sur Internet pour défaut de paiement de ses impôts. L'intéressé allègue que la publication de son nom et d'autres détails sur le site internet de l'administration fiscale pour son manquement à ses obligations fiscales n'était pas nécessaire dans une société démocratique et a porté atteinte à son droit à la vie privée. Il fait valoir que la raison principale de la politique législative hongroise consistant à rendre les données disponibles était l'humiliation publique.

Dans son arrêt de chambre du 12 janvier 2021, la Cour, par cinq voix contre deux, a conclu à la non-violation de l'article 8 de la Convention. Dans les circonstances de l'espèce, la chambre a estimé, en particulier, que rendre publique l'information en cause ne saurait s'analyser en une intrusion grave dans la vie privée du requérant. Elle a donc jugé que la publication de ses données personnelles n'avait pas constitué une atteinte à la vie privée supérieure à ce qui était nécessaire pour protéger l'intérêt légitime de l'État.

<sup>15</sup>. Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 de la Convention.

Le 31 mai 2021, le Collège de Grande Chambre a [accepté](#) la demande de renvoi de l'affaire devant la Grande Chambre présentée par le requérant.

Le 3 novembre 2021, la Grande Chambre a tenu une [audience](#) dans cette affaire.

### **Casarini c. Italie (n° 25578/11)**

Requête communiquée au gouvernement italien le 8 février 2021

Cette affaire concerne l'absence alléguée de garanties suffisantes contre l'accès abusif aux données personnelles stockées dans la base de données du Service d'information pour les contribuables (*Servizio per le informazioni sul contribuente – Ser.P.I.Co.*).

La Cour a communiqué la requête au gouvernement italien et posé des questions aux parties sous l'angle de l'article 8 et de l'article 35 (conditions de recevabilité) de la Convention.

## Données de prestataires de services de télécommunications

### **Breyer c. Allemagne**

30 janvier 2020

En application des modifications apportées en 2004 à la loi allemande sur les télécommunications, les opérateurs furent placés dans l'obligation de recueillir et de conserver les données personnelles relatives à tous leurs clients, y compris les utilisateurs de cartes SIM prépayées, ce qui n'était pas le cas auparavant. Les requérants, qui militaient pour la défense des libertés publiques et réprouvaient la surveillance opérée par l'État, utilisaient ce type de cartes et durent par conséquent faire enregistrer auprès de leurs opérateurs leurs données personnelles telles que leur numéro de téléphone, leur date de naissance, leur nom et leur adresse. Ils se plaignaient devant la Cour de la conservation de leurs données personnelles dans le cadre de l'utilisation par eux de cartes SIM prépayées.

La Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que l'Allemagne n'avait pas outrepassé les limites de la latitude (« marge d'appréciation ») dont elle jouissait dans l'application de la loi en question, lorsqu'elle avait choisi les moyens d'atteindre les buts légitimes que sont la protection de la sécurité nationale et la lutte contre les infractions pénales, et que la conservation des données personnelles des requérants avait été proportionnée et « nécessaire dans une société démocratique ». La Cour a estimé en particulier que la collecte des noms et adresses des requérants dans le cadre de l'utilisation par eux de cartes SIM prépayées avait constitué une ingérence limitée dans l'exercice de leurs droits. Elle a toutefois observé que la loi pertinente offrait des garanties complémentaires et que, par ailleurs, les justiciables pouvaient saisir des organes indépendants chargés de la protection des données afin qu'ils contrôlent les demandes de données émanant des autorités et, le cas échéant, former un recours.

## Mémorisation dans des registres secrets

### **Leander c. Suède**

23 mars 1987

Cette affaire concernait l'utilisation d'un fichier secret de police pour l'embauche d'un charpentier. Le requérant, qui avait travaillé en remplacement au musée naval de Karlskrona, à côté d'une zone militaire interdite, se plaignait du fait que des données liées à ses activités syndicales passées aient été mémorisées et s'étaient trouvées à l'origine de son exclusion de l'emploi en question. Selon lui, ses antécédents personnels ou politiques ne fournissaient aucune raison qui commandât de l'inscrire dans le registre de la Sûreté et de le cataloguer comme « dangereux pour la sécurité ».

La Cour a conclu à la **non-violation de l'article 8** de la Convention. Relevant en particulier que la mémorisation dans un registre secret et la communication de données relatives à la vie privée d'un individu entrent bien dans le champ d'application de l'article 8 de la Convention, elle a également rappelé que, dans une société démocratique, l'existence de services de renseignement et la conservation des



informations peuvent s'avérer légitimes et prévaloir sur l'intérêt des citoyens, à condition de poursuivre des buts légitimes, à savoir la défense de l'ordre, la prévention des infractions pénales ou la protection de la sécurité nationale. En l'espèce, la Cour a estimé que les garanties dont s'entourait le système suédois de contrôle du personnel remplissaient les exigences de l'article 8 de la Convention et que le gouvernement suédois était en droit de considérer que les intérêts de la sécurité nationale prévalaient sur les intérêts individuels du requérant.

### Rotaru c. Roumanie

4 mai 2000 (Grande Chambre)

Voir ci-dessous, sous « Effacement ou destruction de données personnelles ».

### Turek c. Slovaquie

14 février 2006

Voir ci-dessous sous « Accès aux données personnelles ».

## Procédures en matière d'assurance sociale

### Vukota-Bojić c. Suisse

18 octobre 2016

Victime d'un accident de la route, la requérante demanda par la suite une pension d'invalidité. Dans le cadre d'un litige avec son assureur quant au montant de cette pension, après plusieurs années de contentieux, ce dernier lui demanda de passer un autre examen médical de manière à évaluer à nouveau son état de santé, ce qu'elle refusa. À la suite de cela, il engagea des détectives privés afin de la mettre sous surveillance en secret. Les preuves ainsi recueillies furent produites au cours d'un procès ultérieur, qui se solda par la diminution du montant des prestations offertes à la requérante. Cette dernière estimait que cette surveillance avait été contraire à son droit au respect de sa vie privée et que ces preuves n'auraient pas dû être admises au cours du procès.

La Cour a conclu à la **violation de l'article 8** de la Convention. Elle a jugé en particulier que, l'assureur étant regardé comme une entité publique en droit suisse, son action avait engagé la responsabilité de l'État sur le terrain de la Convention. La Cour a également estimé que, bien qu'elle eût été conduite dans des lieux publics, la surveillance secrète litigieuse avait porté atteinte à la vie privée de la requérante, les enquêteurs ayant collecté et stocké des données de manière systématique et les ayant utilisées à des fins précises. De plus, cette mesure n'avait pas été prévue par la loi, les dispositions de droit suisse sur lesquelles elle était fondée étant insuffisamment précises. En particulier, elles n'indiquaient pas clairement à quel moment et pendant quelle durée la surveillance pouvait être conduite, ni selon quelles modalités les données ainsi recueillies pouvaient être stockées et consultées. La Cour a par ailleurs jugé que l'utilisation des preuves obtenues au moyen de la surveillance dans le litige qui opposait la requérante à son assureur n'avait pas rendu le procès inéquitable et qu'il n'y avait donc pas eu **violation de l'article 6** (droit à un procès équitable) de la Convention en l'espèce. À cet égard, elle a relevé en particulier que la requérante avait dûment eu la possibilité de contester les preuves ainsi recueillies et que les juridictions suisses avaient motivé leurs décisions autorisant l'admission de ces pièces.

### Mehmedovic c. Suisse

11 décembre 2018 (décision sur la recevabilité)

Cette affaire concernait la surveillance d'un assuré (le premier requérant) et, par ricochet, de son épouse dans des lieux publics, par des détectives d'une assurance, dans le but de vérifier si la demande en réparation de l'intéressé, qui faisait suite à la survenance d'un accident, était justifiée.

La Cour a déclaré la requête **irrecevable** pour défaut manifeste de fondement. D'une part, elle a constaté que les investigations de l'assureur, effectuées à partir du domaine public et limitées à la constatation de la mobilité du premier requérant, avaient

visé uniquement à préserver les droits patrimoniaux de l'assurance. À cet égard, la Cour a estimé que les juges nationaux avaient reconnu un intérêt prépondérant à l'assureur et en avaient conclu que l'atteinte à la personnalité de l'intéressé n'avait pas été illicite. D'autre part, la Cour a noté que les informations éparses, recueillies par hasard à propos de la requérante et sans aucune pertinence pour l'investigation, avaient été loin de constituer une collecte systématique ou permanente. Selon la Cour, une ingérence dans la vie privée de l'intéressée n'avait donc pas eu lieu.

## Divulgaration de données personnelles

---

### Z. c. Finlande (n° 22009/93)

25 février 1997

Cette affaire concernait la révélation de la séropositivité de la requérante au cours d'une procédure pénale dirigée contre son mari.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la divulgation de l'identité et de la séropositivité de la requérante dans le texte de l'arrêt de la cour d'appel communiqué à la presse ne se justifiait pas par quelque motif impérieux que ce soit et que la publication de ces informations avait dès lors porté atteinte au droit au respect de la vie privée et familiale de la requérante. La Cour a observé en particulier que le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention et est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général. La législation interne doit donc ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention.

### M. S. c. Suède (n° 20837/92)

27 août 1997

Cette affaire concernait la communication par un service de gynécologie à un organisme de sécurité sociale du dossier médical de la requérante.

La Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que le service de gynécologie avait eu des raisons pertinentes et suffisantes de communiquer à l'organisme de sécurité sociale le dossier médical de la requérante et que la mesure n'avait pas été disproportionnée au but légitime poursuivi, à savoir, en permettant à l'organisme de vérifier si se trouvaient réunies les conditions auxquelles la requérante pouvait bénéficier d'une indemnité pour invalidité professionnelle, protéger le bien-être économique du pays. La mesure litigieuse était en outre soumise à des limitations importantes et assortie de garanties effectives et satisfaisantes contre les abus.

### Peck c. Royaume-Uni

29 janvier 2003

Cette affaire concernait la divulgation dans les médias d'une séquence enregistrée dans la rue par une caméra de télévision en circuit fermé (CTCF) de la mairie, montrant le requérant en train de se trancher les veines.

La Cour a jugé que la divulgation de la séquence litigieuse par le conseil municipal n'avait pas été entourée de garanties suffisantes et avait porté une atteinte disproportionnée et injustifiée à la vie privée du requérant, en **violation de l'article 8** de la Convention. Elle a estimé en particulier que, vu les circonstances de l'espèce, il n'y avait pas de raisons pertinentes et suffisantes propres à justifier que le conseil divulguât directement au public des photographies tirées de la séquence, sans avoir au préalable obtenu le consentement du requérant ou caché son identité, ou qu'il divulguât les images aux médias sans avoir pris des mesures pour s'assurer autant que possible qu'un tel masquage serait effectué par eux. L'objectif que constitue la prévention de la criminalité et le contexte de la divulgation exigeaient en l'espèce une vigilance et un

contrôle particuliers sur ces points. La Cour a également conclu à la **violation de l'article 13** (droit à un recours effectif) de la Convention **combiné avec l'article 8**, jugeant que le requérant n'avait pas disposé d'un recours effectif pour faire état de la violation du droit au respect de sa vie privée.

### **Panteleyenko c. Ukraine**

29 juin 2006

Le requérant se plaignait notamment de la divulgation, lors d'une audience judiciaire, d'informations confidentielles concernant sa santé mentale et son traitement psychiatrique.

La Cour a observé que l'obtention, auprès d'un hôpital psychiatrique, d'informations confidentielles sur la santé mentale du requérant et le traitement psychiatrique qu'il y avait subi ainsi que la divulgation de celles-ci lors d'une audience publique avaient constitué une ingérence dans le droit de l'intéressé au respect de sa vie privée. Elle a conclu à la **violation de l'article 8** de la Convention, relevant notamment que les informations en cause n'étaient pas de nature à influencer l'issue du litige, que la demande de renseignements présentée par le tribunal de première instance au sujet de la santé mentale du requérant était superflue car elle ne portait pas sur des éléments "importants pour l'enquête, l'instruction ou le procès" et qu'elle était par conséquent illégale au regard de la loi de 2000 sur l'assistance médicale psychiatrique.

### **Armonas c. Lituanie et Biriuk c. Lituanie**

25 novembre 2008

En 2001, le plus grand quotidien lituanien publia un article à la une concernant les risques de sida dans une région reculée de Lituanie. En particulier, des membres du personnel médical d'un centre d'aide au sida et d'un hôpital étaient cités comme ayant confirmé que les requérants étaient séropositifs. Il était également indiqué que la seconde requérante, décrite dans l'article comme « une fille facile », avait eu deux enfants naturels avec le premier requérant.

La Cour a conclu à la **violation de l'article 8** de la Convention en raison du plafond très bas des dommages-intérêts alloués aux requérants. Particulièrement préoccupée par le fait que, selon le journal, les informations relatives à la maladie des requérants avaient été confirmées par le personnel médical, elle a observé qu'il était indispensable que le droit interne garantisse la confidentialité des informations concernant les patients et empêche toute divulgation de données personnelles, eu égard tout particulièrement à l'impact négatif de telles divulgations sur la propension d'autres personnes à se soumettre volontairement à des tests de dépistage du HIV et aux traitements appropriés.

### **Avilkina et autres c. Russie**<sup>16</sup>

6 juin 2013

Les requérants étaient une organisation religieuse, le Centre administratif des témoins de Jéhovah en Russie, et trois témoins de Jéhovah. Ils se plaignaient en particulier de la divulgation de leurs dossiers médicaux aux autorités de poursuite russes à la suite de leur refus de subir des transfusions sanguines durant leur séjour dans des hôpitaux publics. Dans le cadre d'une enquête sur la légalité des activités de l'organisation requérante, les autorités de poursuite avaient demandé à tous les hôpitaux de Saint-Pétersbourg de leur signaler les refus de subir des transfusions sanguines opposés par des témoins de Jéhovah.

La Cour a déclaré la requête **irrecevable** (incompatible *ratione personae*) en ce qui concerne l'organisation religieuse requérante, ainsi qu'en ce qui concerne l'une des trois autres requérantes. S'agissant de cette dernière, son dossier médical n'avait pas été divulgué, point qui ne prêtait pas à controverse entre les parties. La Cour a par ailleurs conclu à la **violation de l'article 8** de la Convention en ce qui concerne les deux autres requérantes. Elle a estimé en particulier que la divulgation d'informations médicales

<sup>16</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

confidentielles les concernant n'avait pas répondu à un besoin social impérieux. En outre, en divulguant des informations confidentielles sans en informer les requérantes au préalable et sans leur donner la possibilité de s'opposer à cette mesure, le procureur avait employé pour les besoins de son enquête des moyens par trop coercitifs. Force était donc de constater que les autorités n'avaient fait aucun effort pour ménager un juste équilibre entre, d'une part, le droit des requérantes au respect de leur vie privée et, d'autre part, l'objectif de protection de la santé publique poursuivi par le procureur.

Voir aussi : [Y.Y. c. Russie \(n° 40378/06\)](#), arrêt du 23 février 2016<sup>17</sup>.

### **Radu c. République de Moldova**

15 avril 2014

La requérante, formatrice à l'école de police, se plaignait qu'un hôpital public avait révélé à son employeur des informations médicales à son sujet. Ces informations furent largement propagées sur le lieu de travail de l'intéressée, qui, peu de temps après, subit une fausse couche due au stress. Elle intenta vainement une action en justice contre l'hôpital et l'école de police.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que l'ingérence dans l'exercice du droit au respect de la vie privée dont se plaignait la requérante n'était pas « prévue par la loi » au sens de cet article.

### **Sõro c. Estonie**

3 septembre 2015

Dans cette affaire, le requérant se plaignait de la publication, au journal officiel estonien de 2004, d'informations relatives à l'emploi de chauffeur qu'il avait occupé au service du Comité pour la sécurité de l'État de l'URSS (le KGB) à l'époque soviétique.

La Cour a conclu à la **violation de l'article 8** de la Convention, estimant que la mesure prise à l'égard du requérant n'avait pas été proportionnée aux buts qu'elle poursuivait. La Cour a notamment relevé que les dispositions pertinentes de la législation nationale prévoyaient la publication d'informations sur tous les employés des anciens services de sécurité – même sur les chauffeurs, comme en l'espèce – quelles qu'aient été leurs fonctions passées. En outre, si la loi sur la divulgation était entrée en vigueur trois ans et demi après la déclaration d'indépendance de l'Estonie, la publication d'informations concernant les anciens employés des services de sécurité s'était étendue sur plusieurs années. En l'espèce, les informations concernant le requérant n'avaient été publiées qu'en 2004, près de treize ans après la déclaration d'indépendance, et le danger que le requérant pouvait représenter au moment de la publication du communiqué n'avait pas été évalué. Enfin, si la loi sur la divulgation n'emportait pour le requérant aucune restriction d'activités professionnelles, celui-ci affirmait que ses collègues l'avaient dénigré et qu'il avait été contraint de quitter son emploi. S'il ne s'agissait pas là d'un effet recherché par la loi, cela n'en reflétait pas moins la gravité de l'ingérence subie par le requérant dans son droit au respect de sa vie privée.

### **Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande**

27 juin 2017 (Grande Chambre)

À la suite de la publication par deux sociétés de données fiscales à caractère personnel relatives à 1,2 millions de personnes, les autorités finlandaises estimèrent qu'une telle publication massive de données à caractère personnel était illégale au regard des lois en matière de protection des données, et interdirent de telles publications à l'avenir. Les sociétés concernées alléguèrent que cette interdiction avait emporté violation de leur droit à la liberté d'expression.

La Grande Chambre a conclu, par quinze voix contre deux, qu'il n'y avait **pas eu violation de l'article 10** (liberté d'expression) de la Convention. Elle a relevé en particulier que l'interdiction avait constitué une ingérence dans l'exercice par les sociétés requérantes de leur liberté d'expression. Cependant, elle a estimé qu'il n'y avait pas eu violation de l'article 10 car cette ingérence était prévue par la loi, poursuivait un but

<sup>17</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

légitime de protection de la vie privée d'individus et ménageait un juste équilibre entre le droit à la vie privée et le droit à la liberté d'expression. En l'espèce, la Grande Chambre a souscrit à la conclusion des juridictions internes selon laquelle la publication et la diffusion en masse des données fiscales en question n'avaient pas contribué à un débat d'intérêt général, et n'avaient pas été exercées aux seules fins de journalisme.

Voir aussi : [Samoylova c. Russie](#), arrêt du 14 décembre 2021<sup>18</sup>.

### **Standard Verlagsgesellschaft mbH c. Autriche (n° 3)**

7 décembre 2021

Cette affaire concernait des décisions de justice ayant ordonné au média requérant de révéler les données d'inscription d'utilisateurs qui avaient déposé des commentaires sur le site Web (derStandard.at) de son journal, *Der Standard*. Ces décisions avaient fait suite à la mise en ligne de commentaires ayant semble-t-il associé certaines figures politiques à la corruption ou au mouvement néonazi, notamment. La société requérante avait retiré ces commentaires mais refusé de divulguer des informations sur leurs auteurs.

La Cour a conclu en l'espèce à la **violation de l'article 10** (liberté d'expression) de la Convention, jugeant que les décisions judiciaires en question n'avaient pas été nécessaires dans une société démocratique. La Cour a constaté, en particulier, que les données d'utilisateur n'étaient pas couvertes par la protection des « sources journalistiques » et qu'il n'y avait pas de droit absolu à l'anonymat en ligne. Elle a cependant remarqué que les juridictions nationales n'avaient pas procédé à une mise en balance entre les intérêts des demandeurs en justice et les intérêts de la société requérante à maintenir l'anonymat de ses utilisateurs en vue de favoriser le libre échange des idées et des informations, protégé par l'article 10 de la Convention.

### **Y.G. c. Russie (n° 8647/12)**<sup>19</sup>

30 août 2022<sup>20</sup>

Cette affaire portait sur la collecte de données relatives à la santé, dont celles du requérant, séropositif et souffrant d'hépatite, dans une base de données qui fut proposée à la vente. Le requérant soutenait que les autorités répressives avaient illégalement collecté, conservé et enregistré dans une base de données des données relatives à sa santé, et qu'elles n'avaient pas assuré la confidentialité de ses données ni mené d'enquête effective sur leur divulgation.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que les autorités russes avaient manqué à leur obligation positive d'assurer une protection adéquate du droit du requérant au respect de sa vie privée. Elle a noté en particulier qu'il n'était pas contesté que seules les autorités avaient accès à la plupart des données contenues dans la base de données, telles que les casiers judiciaires et les mesures préventives qui avaient été appliquées, et que, par le passé, dans le cadre d'une procédure pénale contre le requérant, l'enquêteur en charge avait demandé des informations sur l'état de santé du requérant à l'hôpital des maladies infectieuses. Bien qu'il était contesté que le ministère de l'Intérieur ait constitué la base de données, dans le contexte de l'affaire, il n'y avait pas d'autre explication que le fait que les autorités étatiques, qui avaient accès aux données en question, n'avaient pas réussi à empêcher une atteinte à la confidentialité. En conséquence, ces données sont devenues accessibles au public, engageant ainsi la responsabilité de l'État défendeur. Or les circonstances de cette atteinte majeure à la vie privée n'avaient jamais été élucidées. La Cour a rappelé à cet égard avoir souligné de manière répétée l'importance de garanties appropriées pour empêcher la communication et la divulgation de données en matière de santé.

<sup>18</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

<sup>19</sup>. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

<sup>20</sup>. Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 de la [Convention](#).

## Accès aux données personnelles

---

### Gaskin c. Royaume-Uni

7 juillet 1989

Le requérant, pris en charge par les services sociaux pendant son enfance, chercha à connaître son passé à sa majorité pour surmonter ses problèmes personnels. L'accès à son dossier lui fut refusé au motif qu'il contenait des informations confidentielles.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que les procédures suivies n'avaient pas assuré à la vie privée et familiale du requérant le respect voulu par cet article. Elle a observé en particulier que les personnes se trouvant dans la situation du requérant ont un intérêt primordial, protégé par la Convention, à recevoir les renseignements nécessaires pour connaître et comprendre leur enfance et leurs années de formation. Cependant, le caractère confidentiel des dossiers officiels revêt de l'importance si l'on souhaite recueillir des informations objectives et dignes de foi et peut être nécessaire pour préserver des tiers. Sous ce dernier aspect, un système subordonnant l'accès aux dossiers à l'acceptation des informateurs, comme alors au Royaume-Uni, peut en principe être tenu pour compatible avec l'article 8, eu égard à la marge d'appréciation de l'État. La Cour a toutefois estimé qu'un tel système doit sauvegarder, quand un informateur n'est pas disponible ou refuse abusivement son accord, les intérêts de quiconque cherche à consulter des pièces relatives à sa vie privée et familiale et qu'il ne cadre avec le principe de proportionnalité que s'il charge un organe indépendant, au cas où un informateur ne répond pas ou ne donne pas son consentement, de prendre la décision finale sur l'accès. Or, il n'en allait pas ainsi en l'espèce.

### Odièvre c. France

13 février 2003 (Grande Chambre)

La requérante fut abandonnée à sa naissance aux services de l'Assistance publique par sa mère qui demanda le secret de son identité vis-à-vis de son enfant. Elle se plaignait de ne pouvoir obtenir communication d'éléments identifiants sur sa famille naturelle. Elle dénonçait notamment le lourd préjudice qui en résultait pour elle dans la mesure où elle était privée de la possibilité de réécrire son histoire personnelle.

Dans son arrêt de Grande Chambre, la Cour a observé que la naissance, et singulièrement les circonstances de celle-ci, relève de la vie privée de l'enfant, puis de l'adulte, garantie par l'article 8 de la Convention. Elle a conclu en l'espèce à l'**absence de violation de l'article 8** de la Convention, estimant notamment que la requérante avait eu accès à des informations non identifiantes sur sa mère et sa famille biologique lui permettant d'établir quelques racines de son histoire dans le respect de la préservation des intérêts des tiers. Par ailleurs, une nouvelle loi adoptée en 2002 offrait la possibilité de lever le secret de l'identité et avait mis en place un organe spécifique qui facilitera la recherche des origines biologiques. Cette nouvelle loi pouvait désormais permettre à la requérante de solliciter la réversibilité du secret de l'identité de sa mère sous réserve de l'accord de celle-ci, de manière à assurer équitablement la conciliation entre la protection de cette dernière et la demande légitime de la requérante. La législation française tentait ainsi d'atteindre un équilibre et une proportionnalité suffisante entre les intérêts en cause.

### Roche c. Royaume-Uni

19 octobre 2005 (Grande Chambre)

Le requérant, militaire dans l'armée britannique, fut renvoyé à la vie civile à la fin des années 1960. Dans les années 1980, il commença à avoir de l'hypertension artérielle puis se mit à souffrir d'hypertension, de bronchopneumopathie et d'asthme. Il fut déclaré invalide. Le requérant soutenait que ses problèmes de santé étaient le résultat de sa participation à des tests sur le gaz moutarde et sur un gaz neurotoxique effectués sous les auspices des forces armées britanniques à Porton Down (Angleterre) dans les années 1960. Il se plaignait en particulier de n'avoir pas eu accès à toutes les informations

pertinentes et appropriées qui lui auraient permis d'évaluer les risques auxquels l'avait exposé sa participation à ces essais.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que, dans l'ensemble, le Royaume-Uni n'avait pas satisfait à l'obligation positive qui lui incombait d'offrir au requérant une procédure effective et accessible qui eût permis à l'intéressé d'avoir accès à l'ensemble des informations pertinentes et appropriées, et ainsi d'évaluer tout risque auquel il avait pu être exposé lors de sa participation aux tests. La Cour a notamment observé que l'on ne saurait exiger d'un individu qui, comme le requérant, a constamment cherché à obtenir la divulgation des documents en question en dehors de tout contentieux, que pour obtenir satisfaction il engage une procédure. Quant aux services d'information et aux études sanitaires, ils avaient débuté près de dix ans après que le requérant se fut lancé dans la recherche de documents et, de plus, après l'introduction de sa requête auprès de la Cour.

### **Turek c. Slovaquie**

14 février 2006

Le requérant alléguait en particulier que la conservation d'un dossier de l'ancien service de sécurité de l'ex-Tchécoslovaquie communiste dans lequel il était inscrit sur la liste des agents de ce service, le refus de lui délivrer un « certificat de sécurité », le fait de le débouter de son action en contestation de cette inscription et les conséquences que ces décisions avaient eues pour lui emportaient violation de son droit au respect de sa vie privée.

La Cour a admis que, en particulier dans une procédure concernant les activités de services de sécurité de l'État, il pouvait y avoir des motifs légitimes de limiter l'accès à certains documents ou autres éléments. Cependant, dans le cas d'une procédure de lustration, cette considération n'était plus guère valable, notamment dans la mesure où, par sa nature même, une telle procédure visait à établir des faits remontant à l'époque communiste et n'était pas directement liée aux fonctions actuelles des services de sécurité. De plus, c'était la légalité des activités des services de sécurité qui était en cause. Dans le cas du requérant, la Cour a observé que les tribunaux internes avaient considéré qu'il était fondamental que le requérant prouvât que l'ingérence litigieuse était contraire aux règles applicables à l'époque pertinente, alors que celles-ci étaient secrètes et que l'intéressé, contrairement aux autorités étatiques, c'est-à-dire le service de renseignements slovaque en l'espèce, n'y avait pas pleinement accès. La Cour a estimé que pareille exigence imposait au requérant une charge irréaliste et excessive, et était contraire au principe d'égalité. Il y avait donc eu **violation de l'article 8** de la Convention à raison de l'absence de procédure par laquelle le requérant aurait pu obtenir la protection de son droit au respect de sa vie privée. La Cour a par ailleurs estimé qu'il n'y avait pas lieu d'examiner séparément les incidences de l'inscription du requérant dans les dossiers de l'ancien service de sécurité de l'État et du certificat de sécurité négatif sur la vie privée de l'intéressé.

### **Segerstedt-Wiberg et autres c. Suède**

6 juin 2006

Dans cette affaire, les requérants demandaient tous en vain à consulter l'intégralité des dossiers les concernant détenus par la Sûreté suédoise. Leurs demandes furent rejetées au motif que le fait de leur donner accès à leurs dossiers pouvait compromettre la prévention des infractions pénales ou la protection de la sécurité nationale.

La Cour a conclu à la **non-violation de l'article 8** de la Convention s'agissant du refus d'informer les requérants de l'intégralité des renseignements conservés à leur sujet dans le fichier de la Sûreté. Rappelant en particulier qu'un refus d'accès intégral à un fichier de police secret au niveau national est nécessaire lorsque l'État peut légitimement craindre que la communication de telles informations risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale et à lutter contre le terrorisme, elle a estimé que l'État suédois, eu égard à l'ample marge d'appréciation dont il disposait, était en droit de considérer que les intérêts de la sécurité nationale et de la lutte contre le terrorisme l'emportaient sur les intérêts des requérants

à être informés de l'intégralité des informations les concernant conservées dans les fichiers de la Sûreté.

### **K.H. et autres c. Slovaquie (n° 32881/04)**

28 avril 2009

Les requérantes, huit femmes d'origine rom, se retrouvèrent dans l'impossibilité de procréer après avoir été traitées dans les services gynécologiques de deux hôpitaux différents. Elles soupçonnaient qu'elles avaient été stérilisées pendant leur séjour dans ces hôpitaux et se plaignaient de n'avoir pas pu obtenir des photocopies de leur dossier médical.

La Cour a conclu à la **violation de l'article 8** de la Convention en ce que les requérantes n'avaient pas été autorisées à photocopier leur dossier médical. Elle a estimé en particulier que les personnes qui, à l'instar des requérantes, souhaitent obtenir des photocopies de documents renfermant des informations à caractère personnel les concernant n'ont pas à devoir expliquer précisément pourquoi elles en ont besoin. Ce serait au contraire à toute autorité détentrice d'éléments de ce type qui ne souhaiterait pas les produire de justifier son refus par des motifs impérieux. Les requérantes ayant obtenu des décisions de justice les autorisant à consulter leurs dossiers médicaux dans leur intégralité, les autorités n'avaient pas justifié par des motifs suffisants l'impossibilité pour les intéressées de faire des photocopies de ces documents. Pour parer au risque d'utilisation abusive des informations médicales, il aurait suffi de mettre en place un dispositif législatif visant à limiter strictement les cas dans lesquels celles-ci peuvent être utilisées ainsi que le nombre de personnes pouvant y avoir accès. La Cour a constaté en l'espèce que, si la nouvelle loi sur la santé de 2004 répondait à cette exigence, son entrée en vigueur était trop tardive pour avoir une incidence sur la situation des requérantes en l'espèce.

### **Haralambie c. Roumanie**

27 octobre 2009

Le requérant dénonçait notamment des entraves à son droit d'accès au fichier constitué à son sujet par les anciens services secrets à l'époque communiste.

La Cour a conclu à la **violation de l'article 8** de la Convention, en raison des difficultés opposées au requérant pour consulter le fichier établi à son sujet par les services secrets sous le régime communiste. Elle a jugé que ni la quantité de fichiers transférés ni la défaillance du système d'archivage ne justifiaient un retard de six ans pour accéder à sa demande. Dans cette affaire la Cour a notamment rappelé l'intérêt primordial pour les personnes faisant l'objet de fichiers personnels détenus par les pouvoirs publics de pouvoir y accéder et a souligné que les autorités se doivent de leur offrir une procédure effective d'accès à ces informations.

Voir aussi : **Jarnea c. Roumanie**, arrêt du 19 juillet 2011 ; **Antoneta Tudor c. Roumanie**, arrêt du 24 septembre 2013.

### **Godelli c. Italie**

25 septembre 2012

Cette affaire concernait le secret de la naissance et l'impossibilité pour une personne abandonnée par sa mère d'obtenir des éléments non identifiants sur sa famille naturelle. La requérante dénonçait le lourd préjudice associé à cette méconnaissance de son histoire personnelle, n'ayant pu faire établir, dans le respect de la préservation des intérêts des tiers, aucune racine de son histoire.

La Cour a conclu à la **violation de l'article 8** de la Convention, estimant notamment qu'un juste équilibre n'avait pas été ménagé entre les intérêts en présence, la législation italienne ne permettant pas à un enfant adopté et non reconnu à la naissance, une fois que la mère a décidé de garder l'anonymat, de demander soit des informations non identifiantes sur ses origines, soit la réversibilité du secret de la naissance avec accord de la mère biologique.



### **Magyar Helsinki Bizottság c. Hongrie**

8 novembre 2016 (Grande Chambre)

Cette affaire concernait le refus des autorités de transmettre à une ONG des informations relatives aux avocats commis d'office, les autorités ayant qualifié ces informations de données à caractère personnel non soumises à divulgation selon le droit hongrois. L'ONG requérante alléguait que le refus des tribunaux hongrois d'ordonner la communication des informations en question avait emporté violation de son droit d'accès à l'information.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a constaté en particulier que les informations demandées par l'ONG requérante étaient nécessaires pour lui permettre de mener à bien l'étude sur le fonctionnement du système des commissions d'office, qu'elle réalisait en sa qualité d'organisation non gouvernementale de défense des droits de l'homme, afin de contribuer à un débat sur une question présentant un intérêt public évident. Pour la Cour, en refusant l'accès aux informations demandées, les autorités internes avaient entravé l'exercice par l'ONG de sa liberté de recevoir et de communiquer des informations, d'une manière portant atteinte à la substance même de ses droits protégés par l'article 10. La Cour a par ailleurs observé 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 avait été acceptée, car même si cette demande concernait des données à caractère personnel, elle ne portait pas sur des informations se trouvant hors du domaine public. La Cour a également jugé que le droit hongrois, tel qu'interprété par les juridictions internes, excluait toute appréciation sérieuse du respect du droit de l'ONG requérante à la liberté d'expression, estimant qu'en l'espèce, 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. Enfin, la Cour a estimé que les arguments du gouvernement hongrois n'étaient pas suffisants pour démontrer que l'ingérence était « nécessaire dans une société démocratique », et a conclu que, nonobstant la marge d'appréciation de l'État défendeur, il n'y avait pas de rapport raisonnable de proportionnalité entre la mesure litigieuse (refus de fournir le nom des avocats commis d'office et le nombre de fois où ils avaient été commis dans certains ressorts) et le but légitime poursuivi (la protection des droits d'autrui).

*Voir aussi*, parmi d'autres : **Centre for Democracy and the Rule of Law c. Ukraine**, décision sur la recevabilité du 3 mars 2020 ; **Centre for Democracy and the Rule of Law c. Ukraine**, arrêt du 26 mars 2020 ; **Saure c. Allemagne**, décision sur la recevabilité du 19 octobre 2021.

## Effacement ou destruction de données personnelles

---

### **Rotaru c. Roumanie**

4 mai 2000 (Grande Chambre)

Le requérant se plaignait de l'impossibilité de réfuter les données, selon lui contraires à la réalité, détenues dans un dossier à son sujet par le Service roumain des renseignements (SRI). L'intéressé avait été condamné en 1948 à une peine d'emprisonnement d'un an pour avoir exprimé des opinions critiques à l'égard du régime communiste.

La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que la détention et l'utilisation par le SRI d'informations sur la vie privée du requérant n'étaient pas prévues par la loi. La Cour a observé en particulier que des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics. Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne. Elle a ensuite relevé qu'aucune disposition de droit interne ne définissait ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de

données, ni les circonstances dans lesquelles pouvaient être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixait pas de limites quant à l'ancienneté des informations détenues et la durée de leur conservation. Enfin, il n'existait aucune disposition explicite et détaillée de droit interne sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui pouvait être donné aux informations ainsi obtenues. Dès lors, la Cour la Cour a estimé que le droit roumain n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. La Cour a également conclu dans cette affaire à la **violation de l'article 13** (droit à un recours effectif) de la Convention, en raison de l'impossibilité pour le requérant de contester sa détention ou de réfuter la véracité des renseignements en question.

Voir aussi : [Association « 21 Décembre 1989 » et autres c. Roumanie](#), arrêt du 24 mai 2011.

## Textes et documents

---

Voir notamment :

- [Convention \(n° 108\) du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel](#), adoptée à Strasbourg le 28 janvier 1981
  - [Page Internet](#) du Conseil de l'Europe consacrée à la protection des données
  - [Manuel de droit européen en matière de protection des données](#), Agence des droits fondamentaux de l'Union européenne / Conseil de l'Europe, 2014
- 

**Contact pour la presse :**  
Tél. : +33 (0)3 90 21 42 08