



octobre 2024
Cette fiche ne lie pas la Cour et n'est pas exhaustive

Nouvelles technologies

Adresses IP

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

La Cour européenne des droits de l'homme a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la [Convention européenne des droits de l'homme](#). 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.

Requête pendante

Le Marrec c. France (requête n° 52319/22)

Requête communiquée au gouvernement français le 7 mars 2023

Dans le cadre d'un traitement des données de connexion du requérant, qui était bénéficiaire d'une allocation de solidarité sociale, l'organisme gestionnaire (Caisse d'allocations familiales) détecta que ce dernier avait soumis une déclaration trimestrielle des ressources depuis une adresse IP située à l'étranger. Un contrôle de sa situation fut alors entrepris et, à l'issue de celui-ci, le bénéfice de l'allocation lui fut retiré, avec effet rétroactif. L'intéressé se plaint du traitement de ses données de connexion (notamment la géolocalisation de son adresse IP), qu'il estime n'avoir pas été entouré de garanties légales suffisantes, ainsi que de l'absence de réponse des tribunaux nationaux à son grief selon lequel le traitement de ses données de connexion était attentatoire à sa vie privée.

La Cour a communiqué la requête au gouvernement français et posé des questions aux parties sous l'angle de l'article 8 (droit au respect de la vie privée) ainsi que de l'article 6 § 1 (droit à un procès équitable) de la Convention.

Antennes paraboliques

Khurshid Mustafa et Tarzibachi c. Suède

16 décembre 2008

Cette affaire portait sur une décision judiciaire de ne pas prolonger un bail privé en raison du refus des locataires, un couple marié d'origine irakienne ayant trois enfants mineurs, de retirer une antenne parabolique destinée à capter les émissions de télévision de leur pays d'origine. Le propriétaire proposa aux requérants de rester s'ils acceptaient

de retirer l'antenne parabolique, mais ils refusèrent et durent déménager. Devant la Cour, les intéressés soutenaient que leur liberté de recevoir des informations avait été méconnue.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a relevé en particulier que l'antenne parabolique permettait aux requérants et à leurs enfants de recevoir des programmes de télévision en arabe et en farsi diffusés depuis leur pays et leur région d'origine. Les intéressés regardaient notamment les actualités politiques et sociales, ces informations revêtant un intérêt particulier pour eux, une famille d'immigrés qui souhaitaient rester en contact avec la culture et la langue de leur pays d'origine. À l'époque, il n'y avait pas d'autre moyen pour les intéressés d'avoir accès à ces programmes et l'antenne ne pouvait être placée ailleurs. Les informations diffusées par les journaux étrangers et les chaînes de radio ne peuvent en aucun cas être mises sur le même pied que celles diffusées à la télévision. En outre, les inquiétudes exprimées par le propriétaire quant à la sécurité avaient été examinées par les tribunaux nationaux qui avaient conclu que l'installation était sans danger. De surcroît, l'expulsion des requérants de leur domicile avec leurs trois enfants avait été disproportionnée au but poursuivi, à savoir l'intérêt pour le propriétaire de préserver l'ordre et les bons usages dans la maison.

Applications mobiles

Magyar Kétfarkú Kutya Párt c. Hongrie

20 janvier 2020 (Grande Chambre)

Cette affaire portait sur une application mobile qu'un parti politique avait mise à la disposition des électeurs pour leur permettre, dans le cadre d'un référendum sur l'immigration organisé en 2016, de prendre, publier et commenter anonymement une photographie de leur bulletin de vote nul. Le parti requérant se plaignait d'une violation de ses droits garantis par l'article 10 (droit à la liberté d'expression) de la Convention.

La Grande Chambre a jugé en particulier que la disposition de la loi électorale interne sur laquelle les autorités s'étaient appuyées pour conclure à une violation du principe de l'exercice des droits conformément à leur but n'avait pas permis au parti requérant de prévoir qu'il pourrait être sanctionné pour la mise à disposition de pareille application, qui relève de l'exercice de la liberté d'expression. Compte tenu de l'incertitude considérable qui entourait les effets potentiels de la disposition légale litigieuse appliquée par les autorités internes, elle a conclu que la restriction en cause n'était pas conforme aux exigences découlant de la Convention. En outre, les dispositions en question n'étaient pas formulées avec suffisamment de précision pour exclure tout arbitraire et permettre au parti requérant de régler sa conduite. Il y avait donc eu **violation de l'article 10** (liberté d'expression) de la Convention.

Courrier électronique

Copland c. Royaume-Uni

3 avril 2007

La requérante fut engagée par un établissement d'enseignement postscolaire, un organe établi par la loi et géré par l'État, en qualité d'assistante personnelle du principal. À partir de fin 1995, elle dut travailler en étroite collaboration avec le principal-adjoint. Son utilisation du téléphone, du courrier électronique et d'Internet fut surveillée à l'instigation du principal-adjoint. D'après le gouvernement britannique, cette surveillance visait à vérifier que la requérante n'abusait pas des installations professionnelles à des fins personnelles.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée et de la correspondance) de la Convention. Elle a relevé tout d'abord que les appels téléphoniques passés depuis des locaux professionnels sont de prime abord couverts par les notions de « vie privée » et de « correspondance ». Il s'ensuit logiquement que

les courriers électroniques envoyés depuis le lieu de travail devraient bénéficier d'une protection analogue, tout comme le devraient les renseignements provenant de la surveillance de l'utilisation personnelle d'Internet. En l'espèce, la Cour a estimé que la collecte et la conservation, à l'insu de la requérante, d'informations personnelles concernant son utilisation du téléphone, du courrier électronique et d'Internet avaient constitué une ingérence dans l'exercice par l'intéressée de son droit au respect de sa vie privée et de sa correspondance. Tout en laissant ouverte la question de savoir si la surveillance de l'utilisation faite par un employé du téléphone, du courrier électronique ou d'Internet sur son lieu de travail peut passer pour « nécessaire dans une société démocratique » dans certaines situations à la poursuite d'un but légitime, la Cour a conclu qu'en l'absence, à l'époque des faits, de toute loi au niveau interne régissant la surveillance, l'ingérence n'était pas « prévue par la loi ».

Muscio c. Italie

13 novembre 2007 (décision sur la recevabilité)

Le requérant, président d'une association de parents catholiques, avait porté plainte contre X pour avoir reçu, dans sa boîte postale électronique, des courriers non sollicités (« spam ») à caractère obscène. Il se plaignait dans sa requête de ne pas avoir eu des moyens juridiques pour s'opposer à la réception de ces courriers électroniques.

La Cour a déclaré **irrecevable** (manifestement mal fondé) le grief tiré par le requérant de l'**article 8** (droit au respect de la vie privée) de la Convention. Elle a estimé que la réception de communications indésirables peut s'analyser comme une ingérence dans la vie privée. Toutefois, les utilisateurs du courrier électronique, une fois connectés à Internet, ne peuvent plus jouir d'une protection effective de leur vie privée, et s'exposent à la réception de messages indésirables. Dans ce cadre, l'action judiciaire du requérant n'avait aucune chance d'aboutir, les autorités nationales et les fournisseurs d'accès rencontrant des difficultés objectives dans la lutte contre le « spam ». La Cour ne pouvait donc exiger d'efforts supplémentaires de la part de l'État au titre de ses obligations positives découlant de l'article 8 de la Convention.

Benediktssdóttir c. Islande

16 juin 2009 (décision sur la recevabilité)

La requérante soutenait que, en ne lui apportant pas une protection suffisante contre la publication illégale de ses courriers électroniques privés dans les médias, l'Islande avait manqué à assurer le respect de son droit au respect de la vie privée et de la correspondance. Elle alléguait qu'un tiers, dont elle ne connaissait pas l'identité, s'était procuré les courriers électroniques en question, à son insu et sans son consentement, sur un serveur précédemment détenu et exploité par son ancien employeur, qui avait fait faillite. Les messages comprenaient en particulier des citations directes ou des paraphrases de messages échangés entre elle et l'un des anciens collègues du président directeur général d'une société multinationale relativement aux souhaits de celui-ci de trouver un bon avocat pour l'aider à remettre à la police des documents supposément compromettants qu'il avait en sa possession et pour le représenter dans une future procédure en justice contre les dirigeants de ladite multinationale. Il y avait à l'époque en Islande un débat public relatif à des allégations selon lesquelles des personnalités auraient exercé des pressions illégitimes sur le déroulement des plus grandes enquêtes pénales qui aient jamais été menées dans le pays.

La Cour a déclaré la requête **irrecevable** pour défaut manifeste de fondement. Elle a jugé que rien n'indiquait que les autorités islandaises aient outrepassé leur marge d'appréciation et manqué à ménager un juste équilibre entre le droit à la liberté d'expression du journal, garanti par l'article 10 de la Convention, et le droit de la requérante au respect de sa vie privée et de sa correspondance garanti par l'article 8 de la Convention.

Helander c. Finlande

10 septembre 2013 (décision sur la recevabilité)

Cette affaire portait sur la plainte d'un détenu, l'administration carcérale ayant refusé de lui faire suivre un message à caractère juridique que son avocat avait envoyé à l'adresse électronique officielle de la prison.

La Cour a déclaré la requête **irrecevable** pour défaut manifeste de fondement, dans la mesure où l'avocat du requérant avait immédiatement été informé que son courriel ne serait pas transmis à son client, et que lui-même et son client avaient toujours été en mesure de communiquer rapidement au moyen du téléphone, de lettres ou de visites en personne. Par ailleurs, la Cour a reconnu que la législation finlandaise actuelle ne permet pas de garantir la confidentialité des échanges avocat-client par courriels, et que l'administration carcérale avait donc une raison sérieuse de ne pas faire suivre le message.

Sérvulo & Associados - Sociedade de Advogados, RL c. Portugal

3 septembre 2015

Voir ci-dessous, sous « Données électroniques ».

M.P. c. Portugal (n° 27516/14)

7 septembre 2021

L'ex-mari de la requérante avait accédé à des messages électroniques qu'elle avait échangés sur un site de rencontres et il les avait produits, sans son consentement, dans le cadre, d'une part, d'une procédure qu'il avait engagée en vue de la répartition de l'autorité parentale et, d'autre part, d'une procédure de divorce. Le tribunal aux affaires familiales n'avait finalement pas tenu compte de ces messages. La requérante se plaignait du fait que les juges n'avaient pas sanctionné son mari pour les avoir divulgués.

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, jugeant que l'État portugais s'était acquitté de l'obligation positive qui lui incombait de garantir les droits de la requérante au respect de sa vie privée et au secret de sa correspondance. Elle a observé, en particulier, que les effets de la divulgation des messages litigieux sur la vie privée de la requérante avaient été limités, ces messages n'ayant été divulgués que dans des procédures civiles dans le cadre desquels l'accès du public aux dossiers de ce type de procédures était restreint. La Cour a noté aussi que les messages en question n'avaient pas été examinés concrètement, le tribunal aux affaires familiales n'ayant finalement pas statué sur le fond des demandes formulées par le mari. Pour la Cour, les autorités portugaises avaient mis en balance les intérêts en jeu en respectant les critères établis dans sa jurisprudence. En outre, dès lors que la requérante avait renoncé à toute prétention civile dans le cadre de la procédure pénale, seule restait à trancher la question de la responsabilité pénale du mari, question sur laquelle la Cour ne saurait statuer.

Données électroniques

S. et Marper c. Royaume-Uni

4 décembre 2008 (Grande Chambre)

Cette affaire portait sur la rétention indéfinie dans une base de donnée des empreintes digitales et données ADN (échantillons cellulaires et profil ADN¹) 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** (droit au respect de la vie privée) de la Convention. Elle a considéré notamment que l'usage des techniques scientifiques modernes dans le système de la justice pénale ne pouvait être autorisé à n'importe quel

¹. 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.

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

Cette affaire portait sur l'inscription dans la base de données nationale des délinquants sexuels de trois hommes reconnus coupables de viol sur mineurs de quinze ans par personne ayant autorité.

La Cour a conclu à la **non-violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a estimé que la durée de conservation des données (30 ans au maximum) n'était pas disproportionnée au regard du but poursuivi par la mémorisation des informations, à savoir la prévention des infractions pénales. Elle a relevé qu'en outre, la consultation de ces données était exclusivement accessible à des autorités (tribunaux, police et autorités administratives) astreintes à une obligation de confidentialité, et dans des circonstances précisément déterminées.

Shimovolos c. Russie²

21 juin 2011

Cette affaire portait sur l'enregistrement d'un militant des droits de l'homme dans la « base de données des surveillances », où des informations sur ses déplacements par train et par avion en Russie avaient été consignées, ainsi que son arrestation survenue dans ce contexte.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a observé que la création et la mise à jour de la base de données 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 et a en conséquence estimé que le droit russe 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. La Cour a conclu également dans cette affaire à la **violation de l'article 5** (droit à la liberté et à la sûreté) de la Convention.

Mandil c. France, Barreau et autres c. France et Deceuninck c. France

13 décembre 2011 (décisions sur la recevabilité)

Les requérants étaient des « Faucheurs volontaires » qui avaient participé à l'arrachage de cultures expérimentales de betteraves transgéniques. Le requérant dans la première affaire se plaignait de sa condamnation pénale pour refus de se soumettre à un prélèvement biologique en vue de son inscription sur le fichier national automatisé des empreintes génétiques ; les requérants dans la deuxième affaire estimaient que leur inscription au fichier national automatisé des empreintes génétiques d'une part, et la condamnation pénale pour certains d'entre eux pour refus de se soumettre à un prélèvement biologique d'autre part, avaient constitué une atteinte à leur droit au respect de la vie privée ; le requérant dans la troisième affaire prétendait notamment que l'ordre de prélever des cellules renfermant ses données génétiques avait constitué une atteinte disproportionnée à son intégrité et à sa vie privée.

². Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention européenne des droits de l'homme (« la Convention »).

La Cour a déclaré les requêtes **irrecevables** pour violation de l'obligation de confidentialité des négociations sur un règlement amiable. Elle a estimé que les parties requérantes avaient porté atteinte au principe de la confidentialité édicté par les articles 39 § 2 de la Convention et 62 du Règlement de la Cour et que leur comportement avait constitué un abus du droit de recours individuel au sens de l'article 35 § 3 a) de la Convention.

Robathin c. Autriche

3 juillet 2012

Avocat de son état, le requérant se plaignait d'une perquisition effectuée dans son cabinet en 2006 et de la saisie de documents et de l'ensemble de ses données électroniques dans le cadre d'une procédure pénale dirigée contre lui au motif qu'il était soupçonné d'infractions de vol, de malversation et de fraude commises à l'égard de ses clients. Il fut finalement relaxé sur tous les chefs en 2011.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la correspondance) de la Convention. Elle a observé en particulier que, bien que le requérant ait bénéficié d'un certain nombre de garanties procédurales, la chambre de contrôle devant laquelle il avait porté son affaire n'avait fourni que des motifs très brefs et plutôt généraux lorsqu'elle a autorisé la saisie de l'ensemble des données électroniques du cabinet de l'intéressé, au lieu de la restreindre aux données concernant uniquement la relation entre le requérant et les victimes des infractions alléguées. Or, eu égard aux circonstances spécifiques existant dans un cabinet juridique, des motifs particuliers auraient dû être donnés pour autoriser une perquisition aussi générale. À défaut de tels motifs, la Cour a jugé que la saisie et l'examen de l'ensemble des données avaient dépassé ce qui était nécessaire pour atteindre le but légitime poursuivi.

Bernh Larsen Holding As et autres c. Norvège

14 mars 2013

Dans cette affaire, trois sociétés norvégiennes se plaignaient d'une décision par laquelle l'administration fiscale leur avait enjoint de remettre à ses inspecteurs une copie de l'intégralité des données du serveur informatique qu'elles partageaient. Elles alléguaient en particulier que la mesure litigieuse était entachée d'arbitraire.

La Cour a conclu à la **non-violation de l'article 8** (droit au respect du domicile et de la correspondance) de la Convention. Elle a souscrit à la conclusion des juridictions norvégiennes selon laquelle des raisons d'efficacité s'opposent à ce que le champ d'action de l'administration fiscale soit limité par le fait qu'un contribuable utilise un système d'archivage partagé, même si celui-ci contient des données appartenant à d'autres contribuables. En outre, des garanties contre les abus ont été mises en place.

M.K. c. France (n° 19522/09)

18 avril 2013

Le requérant, qui avait fait l'objet de deux enquêtes pour vol à l'issue desquelles il fut dans un cas relaxé, dans l'autre non poursuivi, se plaignait du fait que ses empreintes digitales avaient été conservées dans un fichier par les autorités françaises.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a estimé, au vu des circonstances de l'espèce, que la conservation de ces données s'analysait en une atteinte disproportionnée au droit du requérant au respect de sa vie privée.

Youth Initiative For Human Rights c. Serbie

25 juin 2013

Cette affaire portait sur l'accès à des informations obtenues par le service serbe de renseignement au moyen de la surveillance électronique. L'ONG requérante se plaignait que le refus du service de renseignement de lui fournir les informations qu'elle demandait – à savoir des informations sur le nombre de personnes que celui-ci avait placé sous surveillance électronique en 2005 – l'avait empêchée de jouer son rôle de « chien de garde ».

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a estimé que le refus obstiné du service de renseignement de se conformer à une décision définitive et obligatoire lui ordonnant de fournir les informations qu'il avait obtenues était contraire au droit interne et revêtait un caractère arbitraire. Sur le terrain de l'**article 46** (force obligatoire et exécution des arrêts) de la Convention, la Cour a par ailleurs indiqué que la manière la plus simple d'exécuter l'arrêt rendu par elle en l'espèce consisterait à faire en sorte que le service de renseignement fournisse à l'ONG requérante les informations réclamées concernant le nombre de personnes ayant fait l'objet d'une surveillance électronique en 2005.

Nagla c. Lettonie

16 juillet 2013

Cette affaire portait sur la perquisition par la police du domicile d'une journaliste connue de la télévision et la saisie de dispositifs de stockage de données. Le domicile de l'intéressée fut perquisitionné à la suite d'une émission diffusée en février 2010 et dans laquelle elle avait informé le public d'une fuite d'informations de la base de données du fisc. La requérante se plaignait en particulier que la perquisition de son domicile l'avait contrainte à révéler des informations ayant permis d'identifier une source journalistique. Elle y voyait une violation de son droit de recevoir et de communiquer des informations.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a souligné que le droit des journalistes de taire leurs sources ne saurait être considéré comme un simple privilège, qui leur serait accordé ou retiré en fonction de la licéité ou de l'illicéité des sources, mais qu'il devait être considéré comme un attribut du droit à l'information, à traiter avec la plus grande circonspection. En l'espèce, les autorités d'enquête n'avaient pas correctement mis en balance l'intérêt de l'enquête à l'obtention d'éléments de preuve et l'intérêt public à la protection de la liberté d'expression des journalistes.

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. Les mesures litigieuses avaient constitué une ingérence proportionnée dans le droit des requérants au respect de leur vie privée et avaient été nécessaires dans une société démocratique.

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** (droit au respect de la vie privée) 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.

Sérvulo & Associados - Sociedade de Advogados, RL c. Portugal

3 septembre 2015

Cette affaire portait sur la perquisition et la saisie de documents informatiques et de messages électroniques dans un cabinet d'avocats lors d'une enquête portant sur des soupçons de corruption, de prise illégale d'intérêts, de blanchiment d'argent dans le cadre d'un achat par le gouvernement portugais de deux sous-marins à un consortium allemand.

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. Elle a estimé qu'en dépit de l'étendue des mandats de perquisition et de saisie, les garanties offertes aux requérants pour prévenir les abus, l'arbitraire et les atteintes au secret professionnel des avocats avaient été adéquates et suffisantes. La perquisition et les saisies n'avaient donc pas porté une atteinte disproportionnée au but légitime poursuivi. La Cour a observé en particulier que, après visualisation des documents informatiques et messages électroniques qui avaient été saisis, le juge d'instruction du Tribunal central d'instruction criminelle avait ordonné la destruction de 850 fichiers informatiques qu'il avait estimé être de caractère privé, couverts par le secret professionnel ou qui ne concernaient pas directement l'affaire. Aux yeux de la Cour, aucun motif ne permettait de mettre en question l'évaluation à laquelle s'était livré le juge, lequel était intervenu pour contrôler la légalité de la perquisition et des saisies et spécialement protéger le secret professionnel des avocats. Par ailleurs, répondant à l'objection des requérants selon laquelle les fichiers informatiques saisis ne leur auraient pas été restitués, la Cour a relevé que les originaux leur avaient cependant bien été rendus, et qu'il n'existait aucune obligation de restituer les copies, qui pouvaient être conservées pendant le délai de prescription des crimes en cause.

Szabó et Vissy c. Hongrie

12 janvier 2016

Cette affaire portait sur 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** (droit au respect de la vie privée) 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.

Trabajo Rueda c. Espagne

30 mai 2017

Cette affaire portait sur la saisie de l'ordinateur du requérant au motif qu'il contenait des éléments pédopornographiques. L'intéressé soutenait que la saisie et l'examen de son ordinateur par la police avaient constitué une ingérence dans son droit au respect de sa vie privée et de sa correspondance.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a observé tout d'abord que l'accès aux archives de l'ordinateur personnel du requérant par les autorités de police et sa condamnation avaient constitué une ingérence dans le droit de l'intéressé à la vie privée. Cette ingérence était prévue par les dispositions du droit national. Elle poursuivait en outre un but légitime, celui de la « prévention des infractions pénales » ou de la « protection des droits d'autrui ». À cet égard, la Cour a notamment souligné que les « sévices sexuels constituent incontestablement un type odieux de méfaits qui fragilisent les victimes » et que « les enfants et autres personnes vulnérables ont droit à la protection de l'État sous la forme d'une prévention efficace les mettant à l'abri des formes aussi graves d'ingérence dans des aspects essentiels de leur vie privée ». La Cour a cependant jugé que la saisie et l'examen des archives de l'ordinateur par la police, sans autorisation judiciaire préalable, n'avaient pas été proportionnés aux buts légitimes poursuivis et n'avaient pas été « nécessaires dans une société démocratique ». En effet, elle a estimé qu'il était difficile d'apprécier l'urgence qui aurait contraint la police à saisir les archives de l'ordinateur personnel du requérant et à accéder à leur contenu, sans obtenir au préalable l'autorisation judiciaire normalement requise, alors qu'il s'agissait d'un ordinateur retenu par la police et que l'autorisation préalable aurait pu être obtenue relativement rapidement sans entraver l'enquête menée par la police.

Dagregorio et Mosconi c. France

30 mai 2017 (décision sur la recevabilité)

Les requérants étaient 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 portait sur 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.

Aycaguer 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** (droit au respect de la vie privée) 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.

Ivashchenko c. Russie³

13 février 2018

Cette affaire portait sur des copies faites par des douaniers russes des fichiers contenus dans l'ordinateur portable d'un photographe journaliste et dans d'autres outils de stockage.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention jugeant que, dans l'ensemble, le gouvernement russe n'avait pas démontré que la législation et la pratique appliquées en l'espèce avaient fourni des garanties nécessaires contre les abus lorsqu'il s'agit d'appliquer la procédure de prélèvement d'échantillon douanier à des données électroniques contenues dans un appareil électronique.

Libert c. France

22 février 2018

Cette affaire portait sur 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** (droit au respect de la vie privée) 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.

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** (droit au respect de la vie privée) 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.

Buturugă c. Roumanie

11 février 2020

Cette affaire portait sur des allégations de violence conjugale et de violation du secret de la correspondance électronique par l'ex-époux de la requérante, qui dénonçait des défaillances dans le système de protection des victimes de violences de ce type.

³. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

L'intéressée se plaignait en particulier d'un manque d'effectivité de l'enquête pénale concernant les faits de violence conjugale dont elle disait avoir fait l'objet. Elle se plaignait aussi que sa sécurité personnelle n'avait pas été assurée de manière adéquate et elle critiquait le refus des autorités d'examiner sa plainte relative à la violation du secret de sa correspondance par son ex-époux.

La Cour a conclu à la **violation des articles 3** (interdiction des traitements inhumains ou dégradants) **et 8** (droit au respect de la vie privée et de la correspondance) de la Convention, en raison des manquements aux obligations positives de l'État découlant de ces articles. Elle a jugé en particulier que les autorités nationales n'avaient pas abordé l'enquête pénale comme soulevant le problème spécifique de la violence conjugale et que, en procédant ainsi, elles n'avaient pas donné une réponse adaptée à la gravité des faits dénoncés par la requérante. L'enquête sur les actes de violence avait été défailante et aucun examen sur le fond de la plainte pour violation du secret de la correspondance, qui était étroitement liée à la plainte pour violences, n'avait été effectué. À cette occasion, la Cour a enfin précisé que la cyberviolence est actuellement reconnue comme un aspect de la violence à l'encontre des femmes et des filles et qu'elle peut se présenter sous diverses formes, dont les violations informatiques de la vie privée, l'intrusion dans l'ordinateur de la victime et la prise, le partage et la manipulation des données et des images, y compris des données intimes.

Gaughran c. Royaume-Uni

13 février 2020

Cette affaire portait sur 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** (droit au respect de la vie privée) 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.

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 renseignement⁴ 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 (droit au respect de la vie privée et de la correspondance), 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 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 avaient 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 communication⁵.

La Grande Chambre a conclu : à l'unanimité, qu'il y avait eu **violation de l'article 8** (droit au respect de la vie privée et de la correspondance) 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

⁴. 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.

⁵. 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.

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 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** (droit au respect de la vie privée, du domicile et de la correspondance) 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.

Nuh Uzun et autres c. Turquie

29 mars 2022

Au moment des faits, les quatorze requérants étaient détenus au sein de différentes prisons en Turquie à la suite de la tentative de coup d'État du 15 juillet 2016, pour appartenance à une organisation terroriste. L'affaire portait principalement

sur l'enregistrement de la correspondance des requérants, au cours de leur détention, sur le Système Informatique du Réseau Judiciaire National (« UYAP »).

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée / droit au respect de la correspondance) de la Convention, jugeant que l'ingérence dans le droit au respect de la vie privée et de la correspondance des requérants ne pouvait être considérée comme ayant été « prévue par la loi ». Elle a observé, en particulier, que l'enregistrement de la correspondance des détenus et des condamnés sur le système UYAP résultait directement et spécifiquement d'une instruction émise par le ministère de la Justice en octobre 2016, réitérée en mars 2017. Cette instruction était par ailleurs destinée aux procureurs de la République et aux directions des établissements pénitentiaires. Il s'agissait donc de documents internes non publiés, qui étaient en principe dépourvus de force obligatoire vis-à-vis des administrés. Pour la Cour, on ne saurait voir dans un texte de cette nature, édicté en dehors de l'exercice d'un pouvoir normatif, une « loi » d'une « qualité » suffisante au sens de la jurisprudence de la Cour.

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

24 septembre 2024 (décision sur la recevabilité)

Ces deux affaires portaient sur la captation des données des utilisateurs de la solution de communication chiffrée EncroChat – EncroChat était une solution de communication chiffrée par téléphonie mobile, distribuée de façon occulte à plus de 66 000 exemplaires entre 2016 et 2020, dans 122 pays – et leur partage avec les autorités de poursuite britanniques. Les requérants – des ressortissants britanniques, tous deux incarcérés au Royaume-Uni – se plaignaient, notamment, d'une part, de la captation de données effectuée par les autorités françaises sur l'ensemble des terminaux reliés au réseau EncroChat, et, d'autre part, de la transmission aux autorités britanniques des données captées au Royaume-Uni. Ils critiquaient à cet égard la qualité des dispositions législatives relatives à la captation autant que la nécessité de ces ingérences.

Considérant que les requérants dans cette affaire n'avaient pas satisfait à l'exigence d'épuisement des voies de recours internes, la Cour a déclaré leurs requêtes **irrecevables**. Elle a relevé, en particulier, que les données des utilisateurs d'EncroChat avaient été collectées à l'initiative des autorités françaises au moyen d'une mesure de captation ordonnée dans le cadre d'une procédure pénale ouverte par la juridiction interrégionale spécialisée de Lille. Les données concernant les utilisateurs d'EncroChat situés au Royaume-Uni avaient été transmises, en tant qu'éléments de preuves déjà en possession des autorités françaises, en exécution d'une décision d'enquête européenne (DEE) émise par le *Crown Prosecution Service* britannique pour être versées à d'autres dossiers pénaux à titre de preuves. Des données issues de la captation avaient ainsi été produites à l'encontre des deux requérants dans le cadre des poursuites pénales dont ils faisaient l'objet au Royaume-Uni. La Cour a également relevé qu'en application de l'article 694-41 du code de procédure pénale français, les requérants pouvaient demander l'annulation de la mesure d'exécution de la DEE décidée par les autorités britanniques dans les mêmes conditions et selon les mêmes modalités qu'aurait pu le faire une personne mise en examen en France, en faisant valoir qu'ils se trouvaient dans une situation procédurale comparable et que les données transmises étaient issues d'une mesure de captation contraire aux exigences de l'article 8 (droit au respect de la vie privée) de la Convention. En l'espèce, la Cour a conclu que les requérants disposaient, en France, d'une voie de recours permettant de contester de façon effective la mesure de transmission de données prise en exécution de la DEE émise par les autorités britanniques, ainsi que la mesure de captation ayant permis de les collecter. Or, ils n'avaient exercé aucun recours devant les juridictions françaises et ne justifiaient d'aucune circonstance particulière qui les auraient dispensés de le faire.

Voir aussi, notamment :

Ringler c. Autriche

12 mai 2020 (comité – décision sur la recevabilité)

Tretter et autres c. Autriche

29 septembre 2020 (comité – décision sur la recevabilité)

Requêtes pendantes

Association confraternelle de la presse judiciaire c. France et 11 autres requêtes (n^{os} 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, portent sur 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 (droit au respect de la vie privée et de la correspondance), 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.

Droits d'auteur sur des livres ou œuvres musicales

SIA AKKA/LAA c. Lettonie

12 juillet 2016

Cette affaire portait sur un grief relatif à la restriction des droits de propriété intellectuelle d'auteurs d'œuvres musicales. La requérante, une association qui gère les droits de propriété intellectuelle sur les œuvres musicales de nombreux auteurs lettons et étrangers, se plaignait de décisions par lesquelles les juridictions nationales lui avaient ordonné de conclure des accords de licence avec deux entreprises de radio et de fixer les droits de diffusion à un niveau équitable. Elle alléguait notamment que ces décisions avaient restreint les droits exclusifs des auteurs qu'elle représentait de conclure librement des accords de licence pour l'utilisation de leurs œuvres musicales.

La Cour a conclu à la **non-violation de l'article 1** (protection de la propriété) **du Protocole n° 1** à la Convention et à la **non-violation de l'article 6 § 1** (droit à un procès équitable) de la Convention. Elle a jugé en particulier que les autorités lettones avaient ménagé un juste équilibre entre les exigences de l'intérêt public (consistant à ce que les radios obtiennent une licence leur permettant de diffuser légalement les œuvres musicales en question, afin que le public y ait accès) et les droits de la requérante (obtenir une juste rémunération pour l'utilisation d'œuvres musicales). Les décisions de justice interne révélaient un souci de ménager un équilibre entre les intérêts concurrents : les juges avaient observé que des œuvres protégées avaient été diffusées en l'absence de licence valable pendant une longue durée et que cette situation était due dans une certaine mesure au fait que la requérante n'avait pas su négocier efficacement avec les entreprises de radio.

Safarov c. Azerbaïdjan

1^{er} septembre 2022

Le requérant, qui était l'auteur d'un livre sur l'histoire de l'Azerbaïdjan, se plaignait d'une atteinte à la propriété intellectuelle au motif qu'un particulier, sans avoir obtenu son autorisation et sans lui verser de droits d'auteur, avait reproduit son livre et l'avait publié sur Internet. La demande qu'il forma au civil fut rejetée, de même que son pourvoi en cassation. L'intéressé dénonçait un manquement de l'État à son obligation de protéger ses intérêts en matière de propriété intellectuelle et d'un défaut de motivation des décisions rendues par les juridictions internes le concernant.

La Cour a conclu à la **violation de l'article 1** (protection de la propriété) **du Protocole n° 1** à la Convention dans la présente affaire, jugeant que l'État défendeur

avait manqué à l'obligation positive qui lui incombait en vertu de l'article 1 du Protocole n° 1 de protéger la propriété intellectuelle notamment par des mesures de redressement efficaces.

Korotyuk c. Ukraine

19 janvier 2023

Cette affaire portait sur un livre écrit par la requérante – *Commentaire scientifique et pratique de la loi ukrainienne sur les notaires* – mis à disposition sans son consentement en téléchargement payant sur un site en ligne de manuels scolaires. Elle porta plainte à la police en 2013 et l'enquête était apparemment toujours en cours. Devant la Cour, la requérante se plaignait de l'absence d'enquête effective sur le téléchargement illégal de son livre et de l'incapacité de l'État à protéger sa propriété intellectuelle.

La Cour a conclu à la **violation de l'article 1** (protection de la propriété) **du Protocole n° 1** à la Convention dans le cas de la requérante. Elle a relevé en particulier que, même si les litiges portant sur des droits d'auteur étaient en général de nature civile, dans les circonstances particulières de l'espèce, qui concernait des allégations d'infraction pénale, l'État défendeur avait l'obligation positive, au titre de l'article 1 du Protocole n° 1, de mener une enquête pénale effective. À cet égard, la Cour a observé que l'enquête pénale présentait un certain nombre de lacunes. Elle a jugé qu'il résultait du cumul des flagrantes et graves lacunes qui avaient caractérisé l'enquête pénale que l'État avait manqué à ses obligations positives à l'égard des biens de la requérante.

GPS (système de positionnement universel)

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 à la **non-violation de l'article 8** (droit au respect de la vie privée) de la Convention. Compte tenu du fait que l'enquête pénale avait concerné des crimes très graves, elle a jugé que la surveillance par GPS du requérant avait été proportionnée au but poursuivi.

Ben Faiza c. France

8 février 2018

Cette affaire portait sur 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** (droit au respect de la vie privée) 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.

Harcèlement en ligne

Volodina c. Russie (n° 2)⁶

14 septembre 2021

Cette affaire portait sur les allégations de la requérante selon lesquelles les autorités russes auraient manqué à la protéger d'actes répétés de harcèlement en ligne. Elle soutenait, en particulier, que son ancien compagnon aurait utilisé son nom, ses données personnelles et des photos intimes pour créer de faux profils sur des réseaux sociaux, qu'il aurait placé un traceur GPS dans son sac à main, qu'il lui aurait adressé des menaces de mort via les réseaux sociaux et que les autorités n'auraient pas enquêté de manière efficace sur ces allégations.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention, jugeant que les autorités russes avaient failli aux obligations qui leur incombaient au titre de cette disposition de protéger la requérante de graves abus. Elle a relevé, en particulier, que, alors qu'elles disposaient des outils juridiques pour poursuivre le compagnon de la requérante, les autorités n'ont pas enquêté de manière effective et ne se sont, à aucun stade quelconque, interrogées sur ce qui aurait pu ou aurait dû être fait pour protéger la requérante du harcèlement en ligne récurrent.

Interception de radio- ou télécommunications

Roman Zakharov c. Russie⁷

4 décembre 2015

Cette affaire portait sur 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** (droit au respect de la vie privée et de la correspondance) 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

⁶. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

⁷. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

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 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.

Brambilla et autres c. Italie

23 juin 2016

Cette affaire portait sur la condamnation de trois journalistes ayant intercepté des radiocommunications échangées par des gendarmes dans le but de se rendre rapidement sur les lieux d'un crime et de relater les informations dans un journal local.

La Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention. Rappelant la notion de journalisme responsable et relevant que les décisions des juridictions nationales avaient été dûment motivées, notamment en accordant une place primordiale à la défense de la sécurité nationale, de l'ordre et à la prévention du crime, la Cour a jugé en particulier que les juridictions italiennes avaient établi une distinction appropriée entre le devoir des trois journalistes de respecter la loi interne, interdisant de manière générale l'interception par une personne de toute communication qui ne lui est pas adressée dont celles des forces de police, et la poursuite de leur activité journalistique, non limitée en tant que telle. La Cour a également relevé que les sanctions ordonnées par les juridictions internes, consistant en la saisie des appareils-radio et en la condamnation à des peines de privation de liberté, n'avaient pas été disproportionnées, les trois journalistes ayant bénéficié d'une suspension de peine et les autorités ne leur ayant pas interdit de porter à la connaissance du public des faits divers.

Internet⁸

Perrin c. Royaume-Uni

18 octobre 2005 (décision sur la recevabilité)

Cette affaire portait sur la condamnation à 30 mois d'emprisonnement pour publications obscènes sur Internet d'un ressortissant français établi au Royaume-Uni qui exploitait un site internet (détenu par une société qui avait son siège aux États-Unis) montrant des scènes sexuellement explicites.

La Cour a déclaré **irrecevable**, pour défaut manifeste de fondement, le grief tiré par le requérant de l'**article 10** (liberté d'expression) de la Convention. Elle a jugé en particulier que la condamnation pénale de l'intéressé avait été nécessaire dans une société démocratique aux fins de la protection de la morale et/ou des droits d'autrui, et que la peine infligée n'avait pas été disproportionnée.

Paeffgen GmbH c. Allemagne

18 septembre 2007 (décision sur la recevabilité)

Cette affaire portait sur une action introduite contre la société requérante, qui faisait du e-commerce, par d'autres sociétés et par des particuliers qui soutenaient que l'enregistrement et l'utilisation par l'intéressée de différents noms de domaine sur Internet portaient atteinte à leurs droits à la marque et / ou à leurs droits au nom et au nom commercial.

La Cour a déclaré **irrecevable**, pour défaut manifeste de fondement, le grief tiré par le requérant de l'**article 1** (protection de la propriété) **du Protocole n° 1** à la Convention. Elle a jugé que les décisions par lesquelles les juridictions internes avaient ordonné à la société requérante de retirer les domaines litigieux avaient respecté un juste équilibre entre la protection des biens de l'intéressée et les exigences de l'intérêt général

⁸. Voir également la fiche thématique « [Accès à Internet et liberté de communiquer des informations](#) ».

(consistant en l'espèce à mettre fin aux violations des droits à la marque de tiers commises par la société requérante).

K.U. c. Finlande (n° 2872/02)

2 décembre 2008

Cette affaire concernait une annonce à caractère sexuel publiée sur un site de rencontres par internet relativement à un garçon de 12 ans. La législation finlandaise en vigueur au moment des faits⁹ ne permettait pas à la police ni aux tribunaux d'exiger du fournisseur d'accès à Internet (FAI) qu'il divulgue l'identité de la personne qui avait publié l'annonce, et le FAI, s'estimant lié par la confidentialité, refusait de communiquer cette information. La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a considéré que la publication de l'annonce était un acte de nature pénale, et qu'il avait désigné un mineur comme cible pour les pédophiles. Elle a estimé que le législateur aurait dû prévoir un cadre permettant de concilier la confidentialité des services internet avec la défense de l'ordre, la prévention des infractions pénales et la protection des droits et libertés d'autrui, en particulier ceux des enfants et des autres personnes vulnérables.

Times Newspapers Ltd c. Royaume-Uni (nos 1 & 2)

10 mars 2009

La société requérante, propriétaire et éditrice du quotidien *The Times*, alléguait que la règle de droit britannique voulant que chaque consultation d'informations diffamatoires publiées sur Internet puisse donner lieu à une action en diffamation (« la règle relative à la publication sur Internet ») portait atteinte de manière injustifiée et disproportionnée à sa liberté d'expression. En décembre 1999, le *Times* avait publié deux articles prétendument diffamatoires à l'égard d'un particulier. Ces articles avaient été publiés sur le site web du *Times* le jour de leur publication dans la version papier du journal. Au cours de la procédure pour diffamation intentée relativement à cette publication, il fut ordonné au *Times* d'ajouter sur les deux articles de l'archive internet un avertissement indiquant que ces articles faisaient l'objet d'une procédure en diffamation et ne devaient être ni utilisés ni reproduits sans consultation préalable du service juridique de la société requérante.

La Cour a souligné dans cet arrêt que, grâce à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information. Elle a conclu en l'espèce à la **non-violation de l'article 10** (liberté d'expression) de la Convention : étant donné que les archives étaient gérées par le journal lui-même et que les tribunaux nationaux n'avaient pas indiqué que les articles devaient en être retirés purement et simplement, elle a estimé que l'exigence faite au journal de nuancer de manière adéquate la version internet des articles n'avait pas été disproportionnée.

Willem c. France

16 juillet 2009

Cette affaire portait sur l'appel au boycott de produits israéliens par un maire, au moyen notamment d'un message diffusé sur le site internet de la commune. Le maire fut condamné pour provocation à la discrimination.

La Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention. Les motifs avancés par les juridictions françaises pour justifier l'ingérence dans le droit du requérant à la liberté d'expression avaient été « pertinents et suffisants » aux fins de l'article 10 de la Convention. Par ailleurs, l'amende infligée en l'espèce, d'une relative modicité, n'avait pas été disproportionnée au but poursuivi.

⁹. Entre le moment des faits et l'arrêt de la Cour européenne des droits de l'homme, la loi sur l'exercice de la liberté d'expression dans les médias avait établi un cadre juridique.

Renaud c. France

25 février 2010

Le requérant se plaignait d'avoir été condamné pour diffamation et injure publique à l'endroit d'un maire sur le site internet de l'association dont il était président et webmestre.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a considéré que la condamnation du requérant avait été disproportionnée par rapport au but légitime consistant à protéger la réputation et les droits d'autrui.

Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine

5 mai 2011

Cette affaire avait principalement pour objet l'absence de garanties adéquates en droit ukrainien pour les journalistes utilisant des informations tirées d'Internet. Plus particulièrement, elle portait sur une procédure de diffamation dirigée contre un quotidien régional et contre son rédacteur en chef, suite à la publication d'une lettre téléchargée sur Internet dans laquelle il était allégué que les hauts fonctionnaires locaux étaient corrompus et qu'ils avaient des liens avec les chefs d'une organisation criminelle. Les requérants furent condamnés à publier des excuses et à verser la somme de 15 000 hryvnias ukrainiennes (2 394 euros environ), somme à laquelle le plaignant renonça par la suite dans le cadre d'un règlement amiable.

La Cour a conclu que, n'étant pas prévue par la loi, la condamnation du rédacteur-en-chef à publier des excuses avait été **contraire à l'article 10** (liberté d'expression) de la Convention. Elle a conclu également à la **violation de l'article 10** faute de garanties adéquates pour les journalistes utilisant des informations obtenues sur Internet. Notamment, « compte tenu du rôle joué par l'Internet dans le cadre des activités professionnelles des médias ... » et de son importance dans l'exercice du droit à la liberté d'expression en général (...), la Cour [a] consid[éré] que l'absence d'un cadre légal suffisant au niveau interne permettant aux journalistes d'utiliser des informations tirées de l'Internet sans crainte de s'exposer à des sanctions entrave gravement l'exercice par la presse de sa fonction vitale de "chien de garde" (...) » (§ 64 de l'arrêt).

Mosley c. Royaume-Uni

10 mai 2011

Cette affaire portait sur la publication, dans le journal *News of the World* et sur son site internet, d'articles, d'images et de séquences vidéo dévoilant en détail les activités sexuelles de Max Mosley. Le requérant se plaignait que le journal n'ait pas été tenu en droit interne de le prévenir avant la publication de manière à lui permettre d'intenter une action en référé.

La Cour a conclu à la **non-violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a estimé en particulier que la Convention européenne des droits de l'homme n'exige pas des médias qu'ils avertissent à l'avance les personnes au sujet desquelles ils entendent publier des informations.

Ahmet Yıldırım c. Turquie

18 décembre 2012

Cette affaire portait sur la décision d'un tribunal de bloquer l'accès à « Google Sites » qui hébergeait un site internet dont le propriétaire faisait l'objet d'une procédure pénale pour outrage à la mémoire d'Atatürk. Cette mesure de blocage avait pour effet de verrouiller également l'accès à tous les autres sites hébergés par le serveur. Le requérant se plaignait de l'impossibilité d'accéder à son site internet du fait de cette mesure ordonnée dans le cadre d'une affaire pénale qui n'avait aucun rapport ni avec lui, ni avec son site. Il voyait dans cette mesure une atteinte à son droit à la liberté de recevoir et communiquer des informations et des idées.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a estimé que la mesure en cause avait eu des effets arbitraires et que le contrôle juridictionnel du blocage d'accès n'avait pas réuni les conditions suffisantes pour éviter les abus.

Ashby Donald et autres c. France

10 janvier 2013

Cette affaire portait sur la condamnation de photographes de mode pour contrefaçon pour avoir diffusé sans l'autorisation de maisons de haute couture des photographies, prises par l'un des requérants lors de défilés de mode en 2003, sur le site internet d'une société dédiée à la mode et gérée par les deux autres requérants.

La Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention. Dans les circonstances de l'espèce et eu égard à la marge d'appréciation particulièrement importante dont disposent les autorités internes, la nature et la gravité des sanctions infligées aux requérants n'étaient pas telles que la Cour puisse conclure que l'ingérence litigieuse était disproportionnée par rapport au but poursuivi.

Neij et Sunde Kolmisoppi c. Suède

19 février 2013 (décision sur la recevabilité)

Dans cette affaire, deux des cofondateurs de « The Pirate Bay », l'un des plus grands sites internet au monde permettant l'échange de fichiers torrents, alléguaient que leur condamnation pour complicité d'infraction à la loi sur le copyright avait méconnu leur liberté d'expression.

La Cour a déclaré la requête **irrecevable** pour défaut manifeste de fondement. Elle a estimé que le partage, ou le fait de faciliter le partage, de ce type de fichiers sur Internet, même de données protégées par le copyright et à des fins lucratives, relève du droit « de recevoir ou de communiquer des informations » au sens de l'article 10 (liberté d'expression) de la Convention. Toutefois, elle a jugé que les juridictions internes avaient procédé à une juste mise en balance des intérêts concurrents en jeu – à savoir le droit des requérants de recevoir et de communiquer des informations et la nécessité de protéger le copyright – lorsqu'elles ont condamné les requérants.

Akdeniz c. Turquie

11 mars 2014 (décision sur la recevabilité)

Cette affaire portait sur une mesure de blocage de l'accès à deux sites internet, au motif que ceux-ci diffusaient des œuvres musicales sans respecter la législation sur les droits d'auteur. Le requérant, qui avait déposé sa requête devant la Cour européenne des droits de l'homme en tant qu'utilisateur des sites en question, dénonçait en particulier une violation de sa liberté d'expression.

La Cour a déclaré la requête **irrecevable** (incompatible *ratione personae*), jugeant que le seul fait que le requérant subisse les effets indirects d'une mesure de blocage concernant deux sites consacrés à la diffusion de la musique ne saurait suffire pour qu'il se voie reconnaître la qualité de « victime » au sens de l'article 34 (droit de requête individuelle) de la Convention. Tout en soulignant que les droits des usagers d'Internet revêtent aujourd'hui une importance primordiale pour les individus, la Cour a néanmoins relevé notamment que les deux sites, qui étaient des sites internet spécialisés dans la diffusion musicale, avaient été bloqués parce qu'ils ne respectaient pas la législation relative aux droits d'auteur. En tant qu'utilisateur de ces sites, le requérant avait bénéficié de leurs services et il ne s'était trouvé privé que d'un moyen parmi d'autres d'écouter de la musique. La Cour a en outre considéré que l'intéressé pouvait sans difficulté accéder à tout un éventail d'œuvres musicales par de multiples moyens sans que cela n'entraîne une infraction aux règles régissant les droits d'auteur.

Delfi AS c. Estonie

16 juin 2015 (Grande Chambre)

Cette affaire est la première dans laquelle la Cour a été appelée à examiner un grief relatif à la responsabilité d'un portail d'actualités sur Internet en raison des commentaires laissés par les internautes sur ce dernier. La société requérante, qui exploitait à titre commercial un portail d'actualités, se plaignait que les juridictions nationales l'aient jugée responsable des commentaires injurieux laissés par ses visiteurs sous l'un de ses articles d'actualités en ligne, qui concernait une compagnie de navigation. À la demande des avocats du propriétaire de la compagnie de navigation, la

société requérante avait retiré les commentaires injurieux environ six semaines après leur publication.

La Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention, jugeant que la décision des juridictions estoniennes de tenir la société requérante pour responsable avait été justifiée et n'avait pas constitué une restriction disproportionnée du droit de l'intéressée à la liberté d'expression. La Grande Chambre a tenu compte du caractère extrême des commentaires en cause, du fait qu'ils avaient été laissés en réaction à un article publié par la requérante sur un portail d'actualités que celle-ci exploitait à titre professionnel dans le cadre d'une activité commerciale, de l'insuffisance des mesures prises par la requérante pour retirer sans délai après leur publication les commentaires injurieux, ainsi que du caractère modéré de la somme (320 euros) que la requérante avait été condamnée à payer.

Cengiz et autres c. Turquie

1^{er} décembre 2015

Cette affaire portait sur le blocage d'accès à *YouTube*, un site web permettant aux utilisateurs d'envoyer, de regarder et de partager des vidéos. Les requérants se plaignaient en particulier d'une atteinte à leur droit à la liberté de recevoir et de communiquer des informations et des idées.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention, jugeant en particulier que les requérants, enseignants dans différentes universités, s'étaient trouvés pendant une longue période dans l'impossibilité d'accéder à *YouTube* et qu'en leur qualité d'utilisateurs actifs, eu égard aux circonstances de l'espèce, ils pouvaient légitimement prétendre que la mesure de blocage avait affecté leur droit de recevoir et de communiquer des informations et des idées. Par ailleurs, la Cour a observé que *YouTube* est une plateforme unique permettant la diffusion d'informations ayant un intérêt particulier, notamment en matière politique et sociale, ainsi que l'émergence d'un journalisme citoyen. La Cour a estimé également que la loi ne permettait pas au juge national de bloquer totalement l'accès à Internet et en l'occurrence à *YouTube* en raison de l'un de ses contenus.

Kalda c. Estonie

19 janvier 2016

Dans cette affaire, un détenu se plaignait du refus des autorités de lui accorder un accès à trois sites internet gérés par l'État et par le Conseil de l'Europe et publiant des informations juridiques. Le requérant alléguait en particulier que l'interdiction qui lui avait été faite en vertu du droit estonien d'accéder à ces sites spécifiques avait emporté violation de son droit de recevoir des informations via Internet et l'avait empêché de mener des recherches juridiques en vue de plusieurs procédures judiciaires qu'il avait engagées.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a jugé en particulier que les États ne sont pas tenus de fournir aux détenus un accès à Internet. Toutefois, si un État contractant accepte d'autoriser un tel accès, il doit alors motiver son refus de donner accès à des sites spécifiques. Dans les circonstances spécifiques de l'espèce, les raisons avancées pour interdire au requérant l'accès aux trois sites internet en question, à savoir des motifs de sécurité et des considérations de coût, ne suffisaient pas à justifier l'ingérence dans l'exercice par l'intéressé de son droit de recevoir des informations. Notamment, les autorités estoniennes avaient déjà pris des mesures de sécurité quant à l'utilisation d'Internet par les détenus au moyen d'ordinateurs spécialement adaptés à cette fin, sous le contrôle des autorités pénitentiaires, et avaient supporté les coûts y afférents. De plus, en réalité, les juridictions nationales ne s'étaient livrées à aucune analyse détaillée des risques en matière de sécurité qui pouvaient découler de l'autorisation d'accès aux trois sites additionnels en question, eu égard au fait que ceux-ci étaient gérés par une organisation internationale et par l'État lui-même.

Voir aussi : **Jankovskis c. Lituanie**, arrêt du 17 janvier 2017.

Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie

2 février 2016

Cette affaire portait sur la responsabilité d'un organe d'autorégulation des prestataires de services de contenu sur Internet et d'un portail d'actualités sur Internet pour des commentaires grossiers et injurieux laissés par des internautes sur leurs sites web à la suite de la publication d'une opinion critiquant les pratiques commerciales trompeuses de deux sites web d'annonces immobilières. Les requérants se plaignaient des décisions rendues à leur encontre par les juridictions hongroises, soutenant que ces décisions faisaient peser sur eux en pratique une obligation de modération de la teneur des commentaires laissés sur leurs sites par les internautes, ce qui, selon eux, allait à l'encontre de l'essence même de la liberté d'expression sur Internet.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a rappelé en particulier que, même s'ils ne sont pas les éditeurs des commentaires au sens traditionnel du terme, les portails d'actualités sur Internet doivent en principe assumer certains devoirs et responsabilités. La Cour a toutefois considéré qu'en l'espèce, lorsqu'ils avaient tranché la question de la responsabilité des requérants, les juges hongrois n'avaient pas dûment mis en balance les droits divergents en cause, à savoir d'une part celui des requérants à la liberté d'expression et d'autre part celui des sites d'annonces au respect de leur réputation commerciale : notamment, ils avaient admis d'emblée que les commentaires étaient illicites car attentatoires à la réputation des sites web d'annonces immobilières.

Dallas c. Royaume-Uni

11 février 2016

Cette affaire portait sur la condamnation de la requérante pour atteinte à l'autorité de la justice (*contempt of court*) parce qu'elle avait effectué sur Internet une recherche sur le procès pénal dans lequel elle siégeait en qualité de juré. La requérante estimait que l'infraction de *common law* d'atteinte à l'autorité de la justice n'était pas suffisamment claire.

La Cour a conclu à la **non-violation de l'article 7** (pas de peine sans loi) de la Convention. Elle a jugé, en particulier, que le critère retenu en l'espèce pour définir l'atteinte à l'autorité de la justice était à la fois accessible et prévisible. La fonction créatrice de droit des tribunaux était restée cantonnée dans des limites raisonnables et le jugement dans le procès de la requérante pouvait passer, dans une large mesure, pour une étape dans la clarification graduelle des règles de responsabilité pénale pour atteinte à l'autorité de la justice par le biais de l'interprétation judiciaire. Toute évolution du droit qui en aurait résulté était conforme à la substance de l'infraction et raisonnablement prévisible.

Pihl c. Suède

7 février 2017 (décision sur la recevabilité)

Le requérant, qui avait fait l'objet d'un commentaire diffamatoire anonyme publié sur un blog en ligne, engagea une action civile à l'encontre de la petite association à but non lucratif qui tenait le blog en cause, arguant que la responsabilité de celle-ci devait être retenue pour le commentaire qui avait été posté par un tiers. Les juridictions suédoises puis le chancelier de la Justice le déboutèrent. Devant la Cour, le requérant reprochait aux autorités de ne pas avoir protégé sa réputation et d'avoir porté atteinte à son droit au respect de la vie privée par leur refus d'imputer une responsabilité à l'association.

La Cour a déclaré la requête **irrecevable** pour défaut manifeste de fondement. Elle a observé en particulier que, dans les affaires telles que la présente, il y avait lieu de ménager un équilibre entre, d'une part, le droit au respect de la vie privée, et, d'autre part, la liberté d'expression accordée aux personnes et aux collectifs de personnes qui gèrent un portail internet. Au vu des circonstances de l'affaire, la Cour a jugé que, en refusant de tenir l'association pour responsable relativement au commentaire anonyme, les autorités nationales avaient ménagé un juste équilibre. En effet, même si le commentaire en cause présentait un caractère offensant, il ne s'assimilait pas à un

discours de haine ni à une incitation à la violence, il avait été posté sur un petit blog tenu par une association à but non lucratif, il avait été retiré le lendemain du jour où le requérant avait déposé une réclamation dans ce sens et il n'était donc resté en ligne que pendant neuf jours environ.

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** (droit au respect de la vie privée et de la correspondance) 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.

M.L. et W.W. c. Allemagne (n^{os} 60798/10 et 65599/10)

28 juin 2018

Cette affaire portait sur le refus de la Cour fédérale de justice d'interdire à trois médias différents le maintien de l'accès sur leurs portails internet à des dossiers de presse concernant la condamnation des requérants pour meurtre d'un acteur connu, mentionnés par leurs noms complets. Les requérants se plaignaient d'une atteinte à leur droit au respect de leur vie privée.

La Cour a conclu à l'absence de **violation de l'article 8** (droit au respect de la vie privée) de la Convention. Elle a partagé en particulier la conclusion de la Cour fédérale allemande qui avait rappelé que les médias ont pour mission de participer à la formation de l'opinion démocratique en mettant à la disposition du public des informations anciennes conservées dans leurs archives. La Cour a également rappelé que la manière de traiter un sujet relève de la liberté journalistique et que l'article 10 (liberté d'expression) de la Convention laisse aux journalistes le soin de décider quels détails doivent être ou non publiés, sous la condition que ces choix répondent aux normes éthiques et déontologique de la profession. L'inclusion dans un reportage d'éléments individualisés, tel le nom complet de la personne visée, constitue un aspect important du travail de la presse, d'autant plus lorsqu'il s'agit d'une procédure pénale ayant suscité un intérêt public considérable que l'écoulement du temps n'a pas fait disparaître. Enfin, la Cour a relevé qu'au cours de leur dernière demande de révision du procès en 2004, les requérants s'étaient eux-mêmes tournés vers la presse à laquelle ils avaient transmis un certain nombre de documents tout en l'invitant à en tenir le public informé. Cette attitude relativisait leur espérance d'obtenir l'anonymisation des reportages en cause ou encore un droit à l'oubli numérique. En conclusion, compte tenu de la marge d'appréciation des autorités nationales lorsqu'elles mettent en balance des intérêts divergents, de l'importance de conserver l'accessibilité à des reportages acceptés comme licites et du comportement des requérants vis-à-vis de la presse, la Cour a estimé qu'il n'y avait pas de raisons sérieuses de substituer son avis à celui de la Cour fédérale de justice.

Savva Terentyev c. Russie¹⁰

28 août 2018

Cette affaire portait sur la condamnation du requérant pour incitation à la haine à la suite de remarques insultantes sur des policiers qu'il avait faites dans un commentaire d'article de blog.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a jugé en particulier que, si le langage employé par le requérant était insultant et choquant, cet élément ne suffisait pas à lui seul à justifier l'ingérence dans son droit à la liberté d'expression. Au lieu de voir dans ces propos un appel à la violence physique contre les policiers, les juridictions internes auraient dû les examiner dans leur contexte général, leur auteur ayant cherché de manière provocante à exprimer sa colère à l'égard de ce qu'il considérait comme des irrégularités policières.

Magyar Jeti Zrt c. Hongrie

4 décembre 2018

Dans cette affaire, la société requérante avait été condamnée pour avoir affiché un hyperlien vers une interview sur YouTube dont il avait été ultérieurement jugé qu'elle avait un contenu diffamatoire. La société requérante soutenait que, en mettant en jeu sa responsabilité parce qu'elle avait affiché sur son site internet l'hyperlien en question, les juridictions internes avaient indûment restreint ses droits.

La Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention. Elle a souligné en particulier l'importance des hyperliens pour le bon fonctionnement d'Internet et les a distingués des modes traditionnels de publication en ce qu'ils dirigent les internautes vers des contenus disponibles au lieu de les fournir. Affinant sa jurisprudence sur ces questions, la Cour a énuméré les éléments à retenir sur le terrain de l'article 10 dans l'analyse de la question de savoir si l'affichage d'un hyperlien peut engager la responsabilité de son auteur et a dit qu'un examen individuel s'imposait dans chaque cas. En l'espèce, la Cour a relevé que le droit interne hongrois prévoyant la responsabilité objective du diffuseur de matériaux diffamatoires excluait la possibilité de tout examen réel du droit de la société requérante à la liberté d'expression alors que les tribunaux auraient dû minutieusement analyser cette question. Une telle responsabilité objective pour affichage d'hyperliens risque en outre de nuire à la circulation des informations en ligne et de dissuader les auteurs et éditeurs d'articles d'en faire usage s'ils ne peuvent pas contrôler les informations vers lesquelles ces liens sont dirigés. Elle peut avoir un effet dissuasif sur la liberté d'expression en ligne. La Cour a dès lors jugé que, globalement, les droits de la société requérante avaient été indûment restreints.

Høiness c. Norvège

19 mars 2019

Cette affaire portait sur le refus des juridictions norvégiennes d'engager la responsabilité civile de l'hébergeur d'un forum sur Internet après la publication sur le forum en question de commentaires vulgaires concernant la requérante. Celle-ci soutenait qu'en ne protégeant pas suffisamment son droit à la protection de sa réputation et en la contraignant à payer des frais de justice d'un montant tel que celui octroyé aux défendeurs dans le cas d'espèce, les autorités avaient porté atteinte à ses droits.

La Cour a conclu à la **non-violation de l'article 8** (droit au respect de la vie privée) de la Convention, jugeant que les droits de la requérante découlant de cette disposition avaient été suffisamment préservés par les juridictions norvégiennes. Elle a considéré en particulier qu'en s'efforçant de ménager un équilibre entre, d'une part, les droits de l'intéressée découlant de l'article 8 et, d'autre part, le droit à la liberté d'expression garanti par l'article 10 de la Convention au portail d'actualités et à l'hébergeur de forums de discussion, les juridictions internes avaient agi dans les limites de leur pouvoir d'appréciation (« marge d'appréciation »). Elle a estimé par ailleurs que les décisions des

¹⁰. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

juridictions nationales concernant les frais de justice accordés aux défendeurs n'avaient pas emporté violation de l'article 8 de la Convention en l'espèce.

Beizaras et Levickas c. Lituanie

14 janvier 2020

Les requérants, deux jeunes hommes qui entretenaient une relation, se plaignaient du refus des autorités lituaniennes d'ouvrir une enquête préliminaire à propos des commentaires haineux qui avaient été publiés sur la page Facebook de l'un d'eux. Ce dernier avait publié sur sa page Facebook une photographie sur laquelle tous deux s'embrassaient, ce qui lui avait valu de recevoir sur Internet des centaines de commentaires haineux, dont certains visaient les personnes LGBT en général et d'autres contenaient des menaces dirigées contre eux personnellement. Les requérants y voyaient une discrimination à raison de leur orientation sexuelle. Ils arguaient en outre que ce refus les avait privés de la possibilité d'obtenir réparation en justice.

La Cour a conclu une **violation de l'article 14** (interdiction de la discrimination) **combiné avec l'article 8** (droit au respect de la vie privée) de la Convention, jugeant que les requérants avaient subi une discrimination à raison de leur orientation sexuelle et que le gouvernement lituanien n'avait fourni aucune raison propre à démontrer que cette différence de traitement était compatible avec les normes de la Convention. La Cour a estimé en particulier que l'orientation sexuelle des requérants avait joué un rôle dans la manière dont leur cas avait été traité par les autorités qui, lorsqu'elles avaient refusé d'ouvrir une enquête préliminaire, avaient exprimé de manière très claire qu'elles réprouvaient le fait que les requérants aient affiché aussi publiquement leur homosexualité. Cette attitude discriminante avait privé les requérants de la protection que le droit pénal leur garantissait contre tout appel non dissimulé à une atteinte à leur intégrité physique et mentale. La Cour a également conclu à une **violation de l'article 13** (droit à un recours effectif) de la Convention au motif que les requérants s'étaient vu refuser l'accès à un recours interne effectif propre à leur permettre de faire valoir leurs griefs.

Vladimir Kharitonov c. Russie, OOO Flavus et autres c. Russie, Bulgakov c. Russie et Engels c. Russie¹¹

23 juin 2020

Ces affaires portaient sur le blocage de sites internet en Russie et, en particulier, différents types de mesures de blocage, à savoir : le blocage « collatéral » (lorsque l'adresse IP bloquée est partagée par plusieurs sites, y compris l'adresse ciblée), le blocage « excessif » (lorsque l'ensemble du site est bloqué en raison d'une seule page ou d'un seul fichier) et le blocage « en gros » (trois médias en ligne avaient été bloqués par le Procureur général pour leur couverture de certaines informations). Les requérants se plaignaient du blocage, selon eux illégal et disproportionné, de l'accès à leurs sites internet et reprochaient aux juridictions russes de ne pas avoir examiné leurs griefs sur le fond.

La Cour a conclu à la **violation de l'article 10** (droit à la liberté d'expression) de la Convention et à la **violation de l'article 13** (droit à un recours effectif) **combiné avec l'article 10**. Elle a souligné en particulier l'importance d'Internet en tant qu'outil essentiel dans l'exercice du droit à la liberté d'expression. La Cour a notamment constaté que les dispositions de la loi russe sur l'information, utilisées pour bloquer les sites internet, avaient produit des effets excessifs et arbitraires et n'avaient pas fourni de garanties appropriées contre les abus.

Société Éditrice de Mediapart et autres c. France

14 janvier 2021

Cette affaire portait l'injonction faite à *Mediapart*, site d'information d'actualités en ligne, son directeur et un journaliste, de retirer du site du journal la publication d'extraits d'enregistrements illicites réalisés au domicile de M^{me} Bettencourt, principale actionnaire

¹¹. Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

du groupe *L'Oréal*. Les requérants alléguaient que l'injonction en question avait porté atteinte à leur droit à la liberté d'expression.

La Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention, jugeant que les motifs invoqués par les juridictions internes avaient été pertinents et suffisants pour démontrer que l'ingérence litigieuse avait été nécessaire dans une société démocratique », et que l'injonction prononcée n'était pas allée au-delà de ce qui était nécessaire pour protéger M^{me} Bettencourt de l'atteinte à son droit au respect de sa vie privée. Elle a observé, en particulier, que malgré le rôle essentiel qui revient aux médias dans une société démocratique, les journalistes ne sauraient en principe être déliés de leur devoir de respecter les lois pénales de droit commun au motif que l'article 10 de la Convention leur offrirait une protection inattaquable. En effet, les atteintes à la vie privée résultant d'une intrusion dans l'intimité des individus commises par des dispositifs techniques d'écoutes, de vidéo ou de photographies clandestines doivent faire l'objet d'une protection particulièrement attentive. La Cour a également relevé que les sites internet sont des outils d'information et de communication qui se distinguent particulièrement de la presse écrite, notamment quant à leur capacité à emmagasiner et à diffuser l'information, et que les communications en ligne et leur contenu risquent bien plus que la presse écrite de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée.

Biancardi c. Italie

25 novembre 2021

Cette affaire, portant sur le « droit à l'oubli », est la première affaire dans laquelle la Cour a statué sur la compatibilité avec l'article 10 (liberté d'expression) de la Convention de la condamnation au civil d'un journaliste pour non-désindexation d'informations publiées sur Internet. Le requérant, ancien rédacteur-en-chef d'un journal en ligne, avait été condamné au civil pour avoir conservé sur le site internet de son journal un article relatant une bagarre dans un restaurant, en donnant des détails sur la procédure pénale ouverte à ce sujet. Les tribunaux nationaux avaient notamment relevé que l'intéressé n'avait pas désindexé les tags de l'article, si bien que n'importe qui pouvait taper dans un moteur de recherche le nom du restaurant ou de son propriétaire et avoir accès à des informations sensibles sur la procédure pénale, alors que le restaurateur avait demandé la suppression de l'article.

Dans la présente affaire, la Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention, jugeant que les décisions des juridictions nationales s'analysaient en une restriction justifiable à la liberté d'expression du requérant – d'autant plus que celui-ci n'avait pas été tenu de retirer définitivement l'article de l'Internet. En particulier, la Cour a observé que non seulement les fournisseurs de moteurs de recherche sur Internet, mais aussi les administrateurs de journaux ou d'archives journalistiques accessibles en ligne, comme le requérant, pouvaient être tenus de désindexer des documents. La Cour a également approuvé les décisions des juridictions internes selon lesquelles l'accès prolongé et aisé aux informations sur la procédure pénale concernant le restaurateur avait porté atteinte à son droit à la réputation.

Wikimedia Foundation, Inc. c. Turquie

1^{er} mars 2022 (décision sur la recevabilité)

Cette affaire portait sur la demande de la Présidence de la télécommunication et de l'informatique de supprimer des pages du site internet de la fondation requérante et sur le blocage de l'intégralité de son site en raison de l'impossibilité technique de ne bloquer que ces quelques pages. La requérante alléguait que le blocage de l'accès à l'intégralité du site web Wikipédia s'analysait en une atteinte injustifiée à son droit à la liberté d'expression et que la procédure de contrôle juridictionnel des mesures de blocage de sites web ne réunissait pas les conditions suffisantes pour éviter les abus. Elle soutenait qu'il n'existait aucune voie de recours effective en droit turc et que le recours individuel

dont elle avait saisi la Cour constitutionnelle était devenu ineffectif étant donné que son activité consistait à publier le contenu des pages de son site en temps utile.

La Cour a déclaré la requête **irrecevable**, jugeant que la requérante avait perdu sa qualité de victime. Elle a rappelé, en particulier, avoir conclu dans de nombreuses affaires relatives à la liberté d'expression que le recours constitutionnel devait être considéré comme une voie de recours à épuiser, au sens de l'article 35 § 1 (conditions de recevabilité) de la Convention, pour de tels griefs. En l'espèce, la Cour a pris note du caractère systémique du problème soulevé. Cependant, elle ne disposait pas d'éléments suffisamment pertinents donnant à penser que la Cour constitutionnelle turque (CCT) n'était pas capable de remédier au problème. En effet, la CCT avait rendu en matière de blocage de sites web plusieurs arrêts qui lui avaient permis d'établir de nombreux critères devant guider les autorités nationales et les juridictions appelées à examiner les mesures de blocage. Dans cette affaire, la Cour a considéré que, par le biais du recours individuel dont elle avait été saisie, la CCT avait reconnu en substance la violation de l'article 10 (liberté d'expression) de la Convention et avait réparé de manière adéquate et suffisante le préjudice subi par la requérante à cet égard.

Xavier Lucas c. France

9 juin 2022

Cette affaire portait sur l'obligation de saisir la cour d'appel par voie électronique, via la plateforme e-barreau. Alors que la cour d'appel avait admis la recevabilité du recours en annulation d'une sentence arbitrale présenté, sur papier, par le requérant au motif que le formulaire informatique mis en ligne ne permettait pas de saisir la nature de ce recours et la qualité des parties, la Cour de cassation jugea au contraire qu'il aurait dû être remis par voie électronique. Le requérant se plaignait d'une atteinte à son droit d'accès à un tribunal, au motif que son recours en annulation avait été rejeté comme irrecevable faute d'avoir été présenté par voie électronique.

La Cour a conclu à la **violation de l'article 6 § 1** (accès à un tribunal) de la Convention, jugeant que le requérant s'était vu imposer une charge disproportionnée qui rompait le juste équilibre entre, d'une part, le souci légitime d'assurer le respect des conditions formelles pour saisir les juridictions et d'autre part le droit d'accès au juge. À l'instar du requérant, qui faisait valoir qu'il lui était matériellement impossible de saisir le recours sur la plateforme e-barreau, la Cour a notamment constaté que la remise par voie électronique du recours en annulation sur e-barreau supposait que l'avocat de l'intéressé complète le formulaire en utilisant des notions juridiques impropres. Elle a relevé, en outre, que le gouvernement français n'avait pas démontré que des informations précises relatives aux modalités d'introduction du recours litigieux se trouvaient à la disposition des utilisateurs. La Cour a considéré en l'espèce qu'en faisant prévaloir le principe de l'obligation de communiquer par voie électronique pour saisir la cour d'appel sans prendre en compte les obstacles pratiques auxquels s'était heurté le requérant pour la respecter, la Cour de cassation avait fait preuve d'un formalisme que la garantie de la sécurité juridique et de la bonne administration de la justice n'imposait pas et qui devait, dès lors, être regardé comme excessif.

Hurbain c. Belgique

4 juillet 2023 (Grande Chambre)

Cette affaire portait sur la condamnation civile du requérant, en tant qu'éditeur responsable du quotidien *Le Soir*, à anonymiser, au nom du « droit à l'oubli », l'archive électronique d'un article mentionnant le nom complet d'un conducteur – responsable d'un accident de la route meurtrier survenu en 1994.

La Cour a conclu à la **non-violation de l'article 10** (liberté d'expression) de la Convention, jugeant que, compte tenu de la marge d'appréciation dont disposent les États, les juridictions belges avaient soigneusement réalisé une mise en balance des droits en présence conforme aux exigences de la Convention, de sorte que l'ingérence dans le droit garanti par l'article 10 découlant de l'anonymisation de l'article dans sa version électronique figurant sur le site internet du journal *Le Soir* avait été réduite au strict nécessaire et pouvait dès lors, dans les circonstances de l'espèce, passer pour

nécessaire dans une société démocratique et proportionnée. La Cour a relevé, en particulier, que les juridictions nationales avaient pris en compte de manière cohérente la nature et la gravité des faits de nature judiciaire relatés dans l'article litigieux, l'absence d'actualité ou d'intérêt historique ou scientifique de celui-ci, ainsi que l'absence de notoriété du conducteur. De plus, elles avaient attaché de l'importance au préjudice grave souffert par le conducteur suite au maintien en ligne de l'article litigieux en libre accès, laquelle était de nature à créer un « casier judiciaire virtuel », eu égard notamment au temps qui s'était écoulé depuis la publication de l'article d'origine. En outre, après un examen des mesures envisageables pour la mise en balance des droits en présence, examen dont l'étendue correspondait aux normes procédurales en vigueur en Belgique, elles avaient conclu que l'anonymisation litigieuse n'avait pas constitué, pour le requérant, une charge exorbitante et excessive, tout en ayant représenté, pour le conducteur, la mesure la plus efficace pour la protection de sa vie privée.

Requêtes pendantes

Akdeniz et Altiparmak c. Türkiye (n° 5568/20)

Requête communiquée au gouvernement turc le 26 août 2020

Cette requête porte sur la restriction d'accès à plus de 600 contenus sur Internet (sites d'information et comptes de réseaux sociaux) par des décisions adoptées en 2015 et en 2016 par l'entité administrative chargée de télécommunications.

La Cour a communiqué la requête au gouvernement turc et posé des questions aux parties sous l'angle des articles 10 (liberté d'expression) et 18 (limitation de l'usage des restrictions aux droits) de la Convention.

Akdeniz et Altiparmak c. Türkiye (n° 35278/20)

Requête communiquée au gouvernement turc le 9 février 2021

Cette requête porte sur la restriction d'accès à 111 contenus sur Internet (sites d'information, sites de vidéos et comptes de réseaux sociaux) par une décision adoptée en octobre 2015 par l'entité administrative chargée de télécommunications.

La Cour a communiqué la requête au gouvernement turc et posé des questions aux parties sous l'angle des articles 10 (liberté d'expression) et 18 (limitation de l'usage des restrictions aux droits) de la Convention.

Technologie de reconnaissance faciale

Glukhin c. Russie¹²

4 juillet 2023

Cette affaire portait sur l'utilisation par les autorités de la technologie de reconnaissance faciale contre le requérant après que celui-ci se fut livré à une manifestation solo dans le métro de Moscou. L'intéressé fut identifié puis localisé grâce à la technologie de reconnaissance faciale après avoir voyagé avec une silhouette en carton grandeur nature d'un manifestant dont le cas avait été largement médiatisé qui brandissait une banderole sur laquelle on pouvait lire : « Je risque jusqu'à cinq ans (...) pour des manifestations pacifiques ». Le requérant soutenait en particulier que sa condamnation administrative et le recours à la technologie de reconnaissance faciale aux fins du traitement de ses données à caractère personnel avaient porté atteinte à son droit au respect de la vie privée et à sa liberté d'expression.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention dans le chef du requérant, jugeant que le traitement des données personnelles biométriques de l'intéressé au moyen de la technologie de reconnaissance faciale dans le cadre d'une procédure pour infraction administrative – qui avait poursuivi d'abord le but de l'identifier à partir des photographies et de la vidéo publiées sur Internet puis celui de le localiser et de l'interpeller alors qu'il voyageait dans le métro

¹². Le 16 septembre 2022, la Fédération de Russie a cessé d'être Partie à la Convention.

de Moscou – n’avait pas répondu à « un besoin social impérieux » et ne pouvait être considéré comme « nécessaire dans une société démocratique ». La Cour a relevé en particulier que les mesures prises contre le requérant avaient revêtu un caractère particulièrement intrusif face à ce qui avait été une manifestation pacifique qui n’avait représenté aucune menace pour la sécurité du public ou des transports. En réalité, à la suite de cette manifestation, le requérant n’avait été poursuivi que pour infraction mineure. La Cour a également conclu dans cette affaire à la **violation de l’article 10** (liberté d’expression) de la Convention, jugeant que les juridictions internes n’avaient pas avancé de « raisons pertinentes ou suffisantes » pour justifier que l’intéressé ait été conduit jusqu’au poste de police, placé en état d’arrestation et condamné.

Téléphone portable

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** (droit au respect de la vie privée) 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.

Requête pendante

Minteh c. France (n° 23624/20)

Requête communiquée au gouvernement français le 31 mai 2021

Cette affaire porte sur la condamnation pénale du requérant, pour avoir refusé de communiquer le code de déverrouillage de son téléphone portable aux policiers durant sa garde à vue.

La Cour a communiqué la requête au gouvernement français et posé des questions aux parties sous l’angle des articles 6 § 1 (droit à un procès équitable) et 8 (droit au respect de la vie privée et de la correspondance) de la Convention.

Utilisation de caméras cachées

Haldimann et autres c. Suisse

24 février 2015

Cette affaire portait sur la condamnation de quatre journalistes pour avoir enregistré et

diffusé l'interview réalisée en caméra cachée d'un courtier en assurance privée, dans le cadre d'un reportage télévisé destiné à dénoncer les mauvais conseils délivrés par les courtiers en la matière. Les requérants se plaignaient que leur condamnation au versement d'amendes pénales avait constitué une ingérence disproportionnée dans leur droit à la liberté d'expression.

La Cour était avec cette affaire pour la première fois saisie d'une requête concernant l'utilisation de caméras cachées par des journalistes afin de sensibiliser le public à un sujet d'intérêt général, la personne enregistrée n'étant pas visée personnellement, mais comme représentant d'une catégorie professionnelle. En l'espèce, la Cour a conclu à la **violation de l'article 10** (liberté d'expression) de la Convention, estimant notamment que l'ingérence dans la vie privée du courtier, qui avait renoncé à s'exprimer sur l'entretien en question, n'avait pas été d'une gravité telle qu'elle devait occulter l'intérêt du public à être informé de malfaçons en matière de courtage en assurances. La Cour a en outre observé également qu'il convenait d'accorder le bénéfice du doute aux requérants quant à leur volonté de respecter les règles de déontologie journalistique définies par le droit suisse puisqu'ils avaient notamment limité l'usage de la caméra cachée.

Bremner c. Turquie

13 octobre 2015

Cette affaire portait sur la diffusion d'un reportage télévisé dans lequel le requérant, qui s'emploie à déployer un prosélytisme évangélique, était montré comme un « marchand de religion étranger » menant des activités secrètes en Turquie. L'intéressé alléguait que la diffusion du reportage et le refus des autorités judiciaires de faire droit à sa demande d'indemnisation avaient porté atteinte à son droit au respect de sa vie privée.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention, jugeant en particulier que la diffusion de l'image non floutée du requérant ne saurait être regardée comme une contribution à un quelconque débat d'intérêt général pour la société quel que soit le degré d'intérêt que porte la société à la question du prosélytisme religieux. En ce qui concerne la méthode utilisée, la Cour a considéré que l'usage d'une technique aussi intrusive et attentatoire à la vie privée que celle de la caméra cachée doit en principe être restreint. Certes, dans certains cas, l'usage de la caméra cachée peut s'avérer nécessaire pour le journaliste lorsque les informations sont difficiles à obtenir par un autre moyen. Toutefois cet outil doit être utilisé dans le respect des règles déontologiques et en faisant preuve de retenue.

Voir aussi :

Erdtmann c. Allemagne

5 janvier 2016 (décision sur la recevabilité)

Vidéosurveillance

Peck c. Royaume-Uni

28 janvier 2003

Dans cette affaire, le requérant, qui souffrait de dépression, se plaignait de la divulgation aux médias d'une séquence filmée par une caméra de télévision en circuit fermé (CTCF) installée dans la rue et qui le montrait marchant seul avec un couteau de cuisine à la main (il tenta par la suite de suicider en se tranchant les veines du poignet, ce que ne montrait pas la séquence de la CTCF), cette démarche ayant eu pour conséquence que des images de lui-même avaient été largement publiées et diffusées. Il dénonçait également l'absence de tout recours interne effectif pour dénoncer cette situation.

La Cour a estimé que la divulgation des séquences litigieuses par la mairie 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** (droit au respect de la vie privée) de la Convention. L'intéressé n'avait en outre pas disposé, à l'époque pertinente, d'un recours effectif qui lui eût permis de se plaindre d'un abus de

confiance, en **violation de l'article 13** (droit à un recours effectif) **combiné avec l'article 8** de la Convention.

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** (droit au respect de la vie privée) 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.

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**, pour défaut manifeste de fondement, le grief de la requérante tiré de l'article 8 (droit au respect de la vie privée) 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. Elle 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.

Riina c. Italie

11 mars 2014 (décision sur la recevabilité)

Le requérant, condamné à la réclusion à perpétuité pour avoir commis des crimes très graves, entre autres association de malfaiteurs de type mafieux et de multiples assassinats, se plaignait de la vidéosurveillance constante dans sa cellule, y compris dans les toilettes. Il affirmait que les recours internes contre ces mesures étaient inefficaces.

La Cour a déclaré la requête **irrecevable** sous l'angle des articles 3 (interdiction des traitements inhumains ou dégradants) et 8 (droit au respect de la vie privée et familiale) de la Convention, jugeant que le requérant n'avait pas épuisé les voies de recours internes à sa disposition pour contester l'application de la mesure de vidéosurveillance.

Vasilică Mocanu c. Roumanie

6 décembre 2016

Cette affaire portait sur les conditions de détention du requérant dans les locaux de la police. Le requérant alléguait également que sa cellule était équipée d'une caméra de vidéosurveillance, fonctionnant en permanence et pouvant le filmer.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention, jugeant que la surveillance du requérant par une caméra, qui se trouvait

dans la cellule où il avait été placé dans les locaux de la police départementale, n'était pas prévue par la loi interne.

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** (droit au respect de la vie privée) 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. A 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.

Gorlov et autres c. Russie¹³

2 juillet 2019

Cette affaire portait sur la mise sous surveillance vidéo permanente de détenus dans leurs cellules au moyen de caméras de télévision en circuit fermé. Les intéressés voyaient en particulier dans la surveillance constante de leurs cellules, parfois par des gardiennes, une violation de leur droit au respect de leur vie privée.

La Cour a conclu à la **violation de l'article 8** (droit au respect de la vie privée) de la Convention, jugeant que la mesure en question n'était pas prévue par la loi. Tout en reconnaissant qu'il pourrait être nécessaire de surveiller certaines zones des établissements pénitentiaires, ou certains détenus sur une base permanente, elle a estimé en particulier que le cadre juridique entourant en Russie la vidéosurveillance permanente n'était pas suffisamment claire, précis et détaillé pour offrir une protection appropriée contre l'ingérence arbitraire des pouvoirs publics dans le droit au respect de la vie privée. La Cour a conclu également, dans le chef de deux des requérants, à la **violation de l'article 13** (droit à un recours effectif) de la Convention **en combinaison avec l'article 8**, jugeant qu'ils n'avaient disposé d'aucune voie de recours interne effective pour exposer leur grief de violation du droit au respect de leur vie privée.

Voir aussi, récemment : **Izmestyev c. Russie**, arrêt du 27 août 2019.

López Ribalda et autres c. Espagne

17 octobre 2019 (Grande Chambre)

Cette affaire portait sur la mise sous vidéosurveillance secrète d'employées, à l'origine de leur licenciement. Celles-ci estimaient inéquitables 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

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

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** (droit au respect de la vie privée) 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.

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