mai 2021
Cette fiche ne lie pas la Cour et n'est pas exhaustive

Surveillance de masse

L'**article 8 (droit au respect de la vie privée et familiale, du domicile et de la correspondance) de la Convention européenne des droits de l'homme** dispose que :

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

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

Pour déterminer si l'ingérence des autorités dans la vie privée ou la correspondance des requérants était nécessaire dans une société démocratique et si un juste équilibre a été ménagé entre les différents intérêts en présence, la Cour européenne des droits de l'homme recherche si cette ingérence était prévue par la loi, si elle poursuivait un/des but(s) légitime(s) et si elle était proportionnée à ce(s) but(s).

Klass et autres c. Allemagne

6 septembre 1978 (arrêt)

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

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

Weber et Saravia c. Allemagne

29 juin 2006 (décision sur la recevabilité)

Les requérants – la première était une journaliste indépendante et le second prenait les messages téléphoniques de l'intéressée et les lui transmettait ensuite – alléguaient en particulier que certaines dispositions de la loi de 1994 sur la lutte contre la criminalité

portant modification de la loi de 1968 portant restriction du secret de la correspondance, des envois postaux et des télécommunications (« la loi G 10 »)[1], telles qu'interprétées et modifiées par la Cour constitutionnelle fédérale dans son arrêt du 14 juillet 1999, avaient emporté violation de leur droit au respect de leur vie privée et de leur correspondance.
La Cour a déclaré les griefs des requérants **irrecevables** pour défaut manifeste de fondement. Eu égard à l'ensemble des dispositions litigieuses de la loi G 10 dans sa teneur modifiée, replacées dans leur contexte législatif, elle a estimé qu'il existait des garanties adéquates et effectives contre les abus éventuels des pouvoirs de surveillance stratégique de l'État. La Cour était donc convaincue que l'Allemagne, dans le cadre de sa marge d'appréciation relativement large en la matière, avait été fondée à considérer l'atteinte au secret des télécommunications résultant des dispositions litigieuses comme nécessaire, dans une société démocratique, à la sécurité nationale et à la prévention des infractions pénales.

Liberty et autres c. Royaume-Uni

1er juillet 2008 (arrêt)

Les requérantes, une organisation britannique et deux organisations irlandaises de protection des libertés civiles, alléguaient que, entre 1990 et 1997, leurs communications par téléphone, par télécopie et par courriel, dont certaines contenaient des informations juridiques couvertes par le secret professionnel et des renseignements confidentiels, avaient été interceptées au moyen d'un dispositif électronique géré par le ministère britannique de la Défense. Elles avaient auparavant contesté la légalité des interceptions alléguées devant la commission compétente en matière d'interception de communications, le *Director of Public Prosecutions* et la commission des pouvoirs d'enquête, en vain.
La Cour a conclu à la **violation de l'article 8** de la Convention, jugeant que, faute d'avoir défini avec la clarté requise l'étendue et les modalités d'exercice du pouvoir d'appréciation considérable conféré aux autorités en matière d'interception et d'analyse des communications à destination ou en provenance de l'étranger, la loi en vigueur à l'époque pertinente n'offrait pas une protection suffisante contre les abus de pouvoir. En particulier, aucune précision sur la procédure applicable à l'examen, la diffusion, la conservation et la destruction des données interceptées n'y figurait sous une forme accessible au public. L'ingérence dans les droits des requérantes tels que garantis par l'article 8 n'était donc pas « prévue par la loi ».

Kennedy c. Royaume-Uni

18 mai 2010 (arrêt)

Soupçonnant la police d'intercepter ses communications concernant une petite entreprise qu'il venait de créer, le requérant porta plainte auprès de la Commission des pouvoirs d'enquête (« la CPE »). Il fut finalement informé en 2005 que ses plaintes n'avaient donné lieu à aucune décision en sa faveur. Autrement dit, soit ses communications n'avaient pas été interceptées, soit la CPE tenait pour licite une interception éventuelle. La CPE ne lui donna aucun autre renseignement. Le requérant dénonçait l'interception alléguée de ses communications.
La Cour a conclu à la **non-violation de l'article 8** de la Convention, jugeant que la législation du Royaume-Uni en matière d'interception de communications internes, combinée avec les précisions apportées par la publication d'un code de déontologie, décrivait avec une clarté suffisante les procédures concernant la délivrance et le fonctionnement des mandats d'interception ainsi que le traitement, la communication et la destruction des données recueillies. En outre, aucun élément n'indiquait qu'il y ait eu

[1]. Les modifications en question étaient destinées à tenir compte de la surveillance stratégique des télécommunications, laquelle visait à recueillir des informations par l'interception de télécommunications en vue de l'identification et de la prévention de dangers graves pour la République fédérale d'Allemagne, par exemple une attaque armée sur son territoire, des attaques terroristes internationales et certaines autres infractions graves. Elles consistèrent notamment à étendre les pouvoirs du service fédéral des renseignements relativement à l'enregistrement des télécommunications au cours d'une surveillance stratégique, à l'utilisation des données à caractère personnel ainsi recueillies et à leur transmission à d'autres autorités.

d'importantes lacunes dans l'application et la mise en œuvre du régime de surveillance. Dès lors, eu égard aux garanties contre une mauvaise utilisation des procédures ainsi qu'aux garanties plus générales offertes par le contrôle de la CPE, les mesures de surveillance litigieuses, pour autant qu'elles aient pu être appliquées au requérant, étaient justifiées sous l'angle de l'article 8 de la Convention.

Roman Zakharov c. Russie

4 décembre 2015 (arrêt – Grande Chambre)

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

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

Voir aussi, concernant des mesures de surveillance secrètes prises dans le cadre de procès pénaux : **Akhlyustin c. Russie**, **Zubkov et autres c. Russie**, **Moskalev c. Russie** et **Konstantin Moskalev c. Russie**, arrêts du 7 novembre 2017.

Szabó et Vissy c. Hongrie

12 janvier 2016 (arrêt)

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

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

recours effectif) de la Convention **combiné avec l'article 8**, rappelant que l'article 13 ne peut être interprété comme exigeant un recours contre l'état du droit interne.

Privacy International et autres c. Royaume-Uni

7 juillet 2020 (décision sur la recevabilité)

Les requérants – une ONG sise à Londres, un prestataire de services internet sis à Londres, une association de « hacktivistes » sise en Allemagne, deux sociétés sises aux États-Unis qui fournissent respectivement des services internet et des services de communication ainsi qu'un prestataire de services internet sis en Corée du Sud – croyaient que, pendant une période indéterminée, leurs systèmes avaient fait l'objet d'une ingérence, désignée familièrement par le terme « hacking », de la part du *Government Communications Headquarters* (GCHQ, service du renseignement électronique) et/ou du *Secret Intelligence Service* (MI6, service du renseignement extérieur) du Royaume-Uni. Ils soutenaient que le pouvoir conféré par l'article 7 de la loi de 1994 sur les services de renseignement[2] était dépourvu de base légale, que cet article ne posait aucune exigence d'autorisation judiciaire, qu'il n'y avait aucune information publique sur la manière dont il pouvait être utilisé pour autoriser une ingérence dans les systèmes, et qu'il n'y avait aucune obligation de filtrer les informations recueillies pour en exclure les données non pertinentes. Ils ajoutaient que la possibilité de saisir la Commission des pouvoirs d'enquête (*Investigatory Powers Tribunal*) ne constituait pas un recours effectif, cette commission ne statuant pas sur les cas relevant de l'article 7 de la loi en question.

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

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

[2]. 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.

[3]. 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

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

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

La Grande Chambre a conclu, par quinze voix contre deux, à la **violation de l'article 8** de la Convention. Elle a jugé, en particulier, que même si les caractéristiques principales du régime suédois d'interception en masse répondaient aux exigences de la Convention relatives à la qualité de la loi, le régime en question souffrait néanmoins de trois carences : l'absence de règle claire concernant la destruction des éléments interceptés qui ne contiennent pas de données à caractère personnel, le fait que ni la loi relative au renseignement d'origine électromagnétique ni aucun autre texte n'énonce

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.

l'obligation de prendre en compte les intérêts liés à la vie privée lorsqu'une décision de partage de renseignements avec des partenaires étrangers est adoptée, et l'absence de contrôle *a posteriori* effectif. Ces carences faisaient que le régime en cause ne satisfaisait pas à l'exigence de « garanties de bout en bout », qu'il excédait la marge d'appréciation accordée aux autorités de l'État défendeur à cet égard et, considéré dans son ensemble, n'offrait pas une protection adéquate et effective contre l'arbitraire et le risque d'abus.

Voir aussi, récemment :

Ringler c. Autriche

12 mai 2020 (comité – décision sur la recevabilité)

Tretter et autres c. Autriche

29 septembre 2020 (comité – décision sur la recevabilité)

Requêtes pendantes

Association confraternelle de la presse judiciaire c. France et 11 autres requêtes (nos 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 et 59621/15)

Requêtes communiquées au gouvernement français le 26 avril 2017

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

La Cour a communiqué les requêtes au gouvernement français et posé des questions aux parties sous l'angle des articles 8 (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.

Textes et documents

Voir notamment :

- **« Protection des données personnelles »**, fiche thématique préparée par l'Unité de la Presse de la Cour
- **Sécurité nationale et jurisprudence de la Cour européenne des droits de l'homme**, rapport préparé par la Division de la recherche de la Cour, 2013

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