Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

OBSERVATOIRE SUR LE CONTENTIEUX EUROPÉEN DES DROITS DE L'HOMME N. 3/2021

1. ARRÊT BIG BROTHER WATCH ET AUTRES DU 25 MAI 2021 C. ROYAUME-UNI

1. Faits

1.Les parties requérantes sont des journalistes et des organisations et des personnes militant pour la défense des libertés civiles et des droits des journalistes. Elles soutiennent que les trois régimes de surveillance mis en place au Royaume-Uni par la loi de 2000 ont emporté violation des articles 8 et 10 de la CEDH. En particulier ces régimes consistaient en l'interception en masse des communications, la réception d'éléments interceptés obtenus auprès de gouvernements et de services de renseignements étrangers, l'obtention de données de communication auprès des fournisseurs de services de communication. Les régimes examinés par la Cour se rapportent à la loi de 2000, remplacée par la suite par une loi de 2016 sur les pouvoirs d'enquête. Les trois requêtes ont été introduites après qu'Edward Snowden, un ancien agent contractuel de l'Agence nationale de sécurité des États-Unis (NSA), eut révélé l'existence de programmes de surveillance et de partage de renseignements mis en place par les services de renseignement des États-Unis et du Royaume-Uni. Les parties requérantes estiment qu'en raison de la nature de leurs activités, leurs communications électroniques et/ou leurs données de communication ont pu être interceptées ou recueillies par les services de renseignement britanniques auprès de fournisseurs de services de communication ou de services de renseignement étrangers tels que la NSA.

2. Droit

2. Quant au fond de l'affaire, la Cour traite en premier lieu la question générale du cadrage juridique de l'interception en masse par les services de renseignement de communications transfrontières, ce sur le terrain spécifique de l'article 8 de la CEDH. A cet égard, elle tient à souligner premièrement ce qui suit.
« À l'époque actuelle, où le numérique est de plus en plus présent, la grande majorité des communications se font sous forme numérique et sont acheminées à travers les réseaux mondiaux de télécommunication de manière à emprunter la combinaison de chemins la plus rapide et la moins chère sans aucun rapport significatif avec les frontières nationales. La surveillance qui ne vise pas directement les individus est par conséquent susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère. Il est donc essentiel autant que difficile de définir des garanties en la matière. Contrairement aux interceptions ciblées, qui sont l'objet d'une part importante de la jurisprudence de la Cour et

qui sont avant tout utilisées dans le cadre d'enquêtes pénales, l'interception en masse est également – et peut-être essentiellement – utilisée pour recueillir des informations dans le cadre du renseignement extérieur et pour détecter de nouvelles menaces provenant d'acteurs connus ou inconnus. Lorsqu'ils agissent dans ce domaine, les États contractants ont légitimement besoin d'opérer dans le secret, ce qui implique qu'ils ne rendent publiques que peu d'informations sur le fonctionnement du système, voire aucune ; en outre, les informations mises à la disposition du public peuvent être formulées en termes abscons et souvent largement différents d'un État à l'autre » (par. 322).

Deuxièmement, la Cour tient à ajouter les remarques suivantes.

« Si les capacités technologiques ont considérablement accru le volume des communications transitant par Internet au niveau mondial, les menaces auxquelles sont confrontés les États contractants et leurs citoyens ont également proliféré. On peut citer, sans être exhaustif, le terrorisme, le trafic de substances illicites, la traite des êtres humains ou encore l'exploitation sexuelle des enfants – activités d'échelle planétaire. Nombre de ces menaces proviennent de réseaux internationaux d'acteurs hostiles qui ont accès à une technologie de plus en plus sophistiquée grâce à laquelle ils peuvent communiquer sans être repérés. L'accès à cette technologie permet également à des acteurs étatiques ou non étatiques hostiles de perturber l'infrastructure numérique, voire le bon fonctionnement des processus démocratiques, au moyen de cyberattaques. Il y a là une menace grave pour la sécurité nationale qui, par définition, n'existe que dans le domaine numérique et ne peut donc être détectée et investiguée qu'à l'aide de moyens numériques. Ainsi, pour se prononcer sur la conformité à la Convention des régimes encadrant dans les États contractants l'interception en masse, technologie précieuse qui permet de détecter les nouvelles menaces de nature numérique, la Cour est appelée à examiner les garanties contre l'arbitraire et les abus qui y sont prévues tout en ne disposant que d'informations limitées sur la manière dont ils fonctionnent » (par. 323).

3.Le décor ayant été ainsi planté, la Cour se penche ensuite sur la question de l'existence d'une « ingérence » dans la vie privée dans des situations d'interceptions en masse par les pouvoirs publics de communications. Quant au procédé de l'interception en masse, elle tient à préciser les points suivants :

- Il s'agit un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance.
- Les régimes d'interception en masse ne sont pas forcément tous conçus exactement sur le même modèle, les différentes étapes du processus ne sont pas nécessairement distinctes et ne répondent pas toujours à un ordre chronologique strict.
- Le procédé suit d'ordinaire divers étapes qui vont de la rétention initiale des communications et des données au partage de ces données avec des tiers.

Selon la Cour l'article 8 s'applique à chacune des étapes décrites ci-dessus. Si l'interception suivie de l'élimination immédiate d'une partie des communications ne constitue pas une ingérence particulièrement importante, l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus d'interception en masse avance. De ce fait, « l'intensité de l'atteinte au droit au respect de la vie privée augmente au fur et à mesure que le processus franchit les différentes étapes » (par. 331).

Quant à la question de savoir si une ingérence peut être justifiée, la Cour rappelle ensuite les principes généraux tels qu'il se dégagent de sa jurisprudence eu égard, notamment, au caractère secret des mesures de surveillance. A cet égard elle relève ce qui suit.

« En matière de surveillance secrète, la « prévisibilité » ne peut se comprendre de la même façon que dans la plupart des autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la « prévisibilité » ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles de recourir à ce type de mesures de manière à ce qu'il puisse adapter sa conduite en conséquence. Cependant, le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. En matière de mesures de surveillance secrète, il est donc indispensable qu'existent des règles claires et détaillées, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. Le droit interne doit être suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique est habilitée à recourir à pareilles mesures. En outre, la loi doit définir l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire » (par. 333).

Une des questions essentielles qui se posent pour évaluer les tenants et les aboutissants d'une surveillance secrète concerne la « qualité de la loi » qui l'autorise. En ce sens, pareille « qualité »

« Implique que le droit national doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont « nécessaires dans une société démocratique », notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus » (par. 335).

Puisque la personne concernée sera nécessairement dans l'impossibilité d'introduire de son propre chef un recours effectif ou de prendre une part directe à quelque procédure de contrôle que ce soit, l'un des aspects majeurs mis en lumière par la Cour concerne les mécanismes existants qui doivent procurer par eux-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. En effet,

« En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le contrôle juridictionnel offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière » (par. 336).

Un autre aspect important est constitué par le fait que les interceptions ciblées et l'interception en masse présentent un certain nombre de différences importantes. Ainsi

« L'interception en masse vise généralement les communications internationales (c'est-à-dire les communications qui traversent physiquement les frontières de l'État), et si l'on ne peut exclure que les communications de personnes qui se trouvent dans l'État qui opère la surveillance soient interceptées et même examinées, dans bien des cas le but déclaré de l'interception en masse est de contrôler des communications qui ne peuvent être contrôlées par d'autres formes de surveillance car elles sont échangées par des personnes se trouvant hors de la compétence territoriale de l'État » (par. 344).

Cela étant, la Cour se doit d'affirmer ce qui suit.

« Comme tout système d'interception, l'interception en masse recèle à l'évidence un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée. Certes, l'article 8 de la Convention n'interdit pas de recourir à l'interception en masse afin de protéger la sécurité nationale ou d' autres intérêts nationaux essentiels contre des menaces extérieures graves, et les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet, cependant la

latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et un certain nombre de garanties doivent être mises en place » (par. 347).
4. Quant à l'approche à adopter dans les affaires relatives à l'interception en masse la Cour s'efforce de préciser les conditions et les garanties qui doivent entourer les mesures y relatives. Elle met en exergue en particulier les points suivants.
- Il est impératif que lorsqu'un État met en œuvre un tel système, le droit interne contienne des règles détaillées prévoyant les circonstances dans lesquelles les autorités peuvent avoir recours à de telles mesures. Le cadre juridique devrait, en particulier, énoncer avec suffisamment de clarté les motifs pour lesquels une interception en masse pourrait être autorisée et les circonstances dans lesquelles les communications d'un individu pourraient être interceptées.
- Dans le contexte de l'interception en masse, la supervision et le contrôle des mesures revêtent une importance d'autant plus grande que le risque d'abus est inhérent à ce type d'interception et que le besoin légitime d'opérer dans le secret signifie inévitablement que, pour des raisons tenant à la sécurité nationale, les États ne sont souvent pas libres de divulguer des informations sur le fonctionnement du système en cause.
- Afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus 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. Il s'agit là en fait de facteurs qui sont, de l'avis de la Cour, des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8.
- L'interception en masse devrait être autorisée par un organe indépendant, c'est-à-dire un organe indépendant du pouvoir exécutif.
- L'organe indépendant chargé d'accorder les autorisations devrait être informé à la fois du but poursuivi par l'interception et des canaux de transmission ou des voies de communication susceptibles d'être interceptés. Cela lui permettrait d'apprécier la nécessité et la proportionnalité de l'opération d'interception en masse ainsi que de vérifier si la sélection des canaux est nécessaire et proportionnée aux buts dans lesquels les activités d'interception sont menées.
- L'utilisation de sélecteurs – et en particulier de sélecteurs forts – est l'une des étapes les plus importantes du processus d'interception en masse puisqu'il s'agit du moment où les communications d'un individu déterminé sont susceptibles d'être ciblées par les services de renseignement.
- Des garanties renforcées devraient s'appliquer lorsque les services de renseignement emploient des sélecteurs forts se rapportant à des personnes identifiables. Les services de renseignement devraient être tenus de justifier – au regard des principes de nécessité et de proportionnalité – l'utilisation de chaque sélecteur fort, et cette justification devrait être consignée scrupuleusement et soumise à une procédure d'autorisation interne préalable comportant une vérification distincte et objective de la conformité de la justification avancée aux principes susmentionnés.
- Chaque stade du processus d'interception en masse – notamment l'autorisation initiale et ses éventuels renouvellements, la sélection des canaux de transmission, le choix et l'application de sélecteurs et de termes de recherche, l'utilisation, la conservation, la

transmission à des tiers et la suppression des éléments interceptés – devrait également être soumis à la supervision d'une autorité indépendante, et cette supervision devrait être suffisamment solide pour circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique ».

- Enfin, toute personne qui soupçonne que ses communications ont été interceptées par les services de renseignement devrait disposer d'un recours effectif permettant de contester la légalité de l'interception soupçonnée ou la conformité à la Convention du régime d'interception.

- La transmission, par un État contractant, d'informations obtenues au moyen d'une interception en masse à des États étrangers ou à des organisations internationales devrait être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et qu'elle devrait être soumise à certaines garanties supplémentaires relatives au transfert lui-même.

Appliquant ces principes dans le cas d'espèce, la Cour souligne d'emblée qu'en principe, plus les motifs sont étendus, plus le risque d'abus est important. Elle constate cependant que le régime mis en place par la loi britannique autorisait manifestement l'interception de communications internationales (c'est-à-dire transfrontières) et que les services de renseignement ne devaient exercer leur pouvoir d'interception que sur les canaux de transmission les plus susceptibles d'acheminer des communications extérieures. Elle considère en définitive que les conditions dans lesquelles des éléments interceptés pouvaient être sélectionnés, utilisés et conservés en vertu du régime découlant de la loi applicable étaient suffisamment « prévisibles » aux fins de l'article 8 de la Convention, et qu'elles offraient des garanties adéquates contre les abus.

S'agissant du transfert hors du Royaume-Uni d'éléments interceptés, la Cour considère ce sui suit.

« Lorsque ces éléments avaient été interceptés conformément au droit interne, leur transmission à un service de renseignement étranger allié ou à une organisation internationale ne pouvait poser problème au regard de l'article 8 de la Convention que si l'État qui avait procédé à l'interception ne s'était pas assuré au préalable que son partenaire avait mis en place, pour le traitement de ces éléments interceptés, des garanties propres à prévenir tout abus ou ingérence disproportionnée et, en particulier, que celui-ci était en mesure de garantir la conservation sécurisée de ces éléments et de restreindre leur divulgation à d'autres parties » (par. 395).

Pour étayer sa conclusion sur le point considéré, la Cour estime que le Commissaire à l'interception des communications exerçait une supervision indépendante et effective sur le fonctionnement du régime institué par la loi. En effet, le Commissaire et ses inspecteurs pouvaient notamment évaluer la nécessité et la proportionnalité d'un grand nombre de demandes de mandat et du choix ultérieur des sélecteurs, et examiner les procédures mises en place pour la conservation, le stockage ainsi que la destruction des communications interceptées et des données de communication associées. Ils pouvaient également adresser des recommandations officielles aux chefs des autorités publiques concernées, lesquelles étaient tenues de rendre compte dans un délai de deux mois des progrès accomplis dans la mise en œuvre de ces recommandations.

Quant au contrôle a posteriori, la Cour relève que ce contrôle était assuré par un organe spécifique (IPT), présidé pendant la période sous examen par un juge de la High Court, lequel offrait un recours juridictionnel solide à toutes les personnes qui pensaient que leurs communications avaient été interceptées par les services de renseignement.

5. En conclusion la Cour admet que l'interception en masse revêt pour les États contractants une importance vitale pour détecter les menaces contre leur sécurité nationale. Cela étant, la Cour rappelle que l'interception en masse recèle un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée. Partant elle estime que

« Dans un État régi par la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8, le régime découlant de (la loi litigieuse), considéré dans son ensemble, ne renfermait pas suffisamment de garanties « de bout en bout » pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus, en dépit des garde-fous qu'il comportait, dont certains ont été jugés solides. Elle relève notamment que ce régime présentait des lacunes fondamentales, à savoir l'absence d'autorisation indépendante, l'absence de mention des catégories de sélecteurs dans les demandes de mandat et le fait que les sélecteurs liés à un individu n'étaient pas soumis à une autorisation interne préalable. Ces insuffisances affectaient non seulement l'interception du contenu des communications, mais aussi l'interception des données de communication associées. Si la supervision indépendante et effective exercée sur le régime par le Commissaire à l'interception des communications et le recours juridictionnel solide que l'IPT offrait à toutes les personnes pensant que leurs communications avaient été interceptées par les services de renseignement constituaient des garanties importantes, celles-ci n'étaient pas suffisantes pour contrebalancer les lacunes mises en évidence » (par. 425).

En conséquence, selon la Cour, la législation interne applicable ne répondait pas à l'exigence de « qualité de la loi » et ne permettait donc pas de circonscrire l' «ingérence» au niveau « nécessaire dans une société démocratique» et qu'il y avait eu violation de l'article 8 à cet égard.

6. D'autres questions ont été abordées par la Cour par rapport à la violation alléguée de l'article 10 de la CEDH concernant notamment la protection des sources des journalistes et la protection garantie par la disposition précitée aux communications couvertes par le secret professionnel, ainsi que par rapport à l'article 8 de la CEDH visant la réception de renseignements provenant de services de renseignement étrangers.

Sur la première de ces questions la Cour admet que si les garanties relatives à la conservation, à la transmission à des tiers et à la destruction des éléments journalistiques confidentiels prévues par le code de conduite en matière d'interception de communications étaient adéquates, toutefois les garanties supplémentaires énoncées dans ce code ne remédiaient pas aux lacunes mises en évidence par la Cour dans son analyse du régime litigieux sous l'angle de l'article 8 de la Convention. En outre, le régime litigieux ne comportait pas de garde-fous suffisants garantissant que, lorsqu'il apparaissait que des communications n'ayant pas été sélectionnées pour examen par l'utilisation délibérée d'un sélecteur ou d'un terme de recherche dont on savait qu'il était lié à un journaliste contenaient malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne seraient possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures étaient « justifiées par un impératif prépondérant d'intérêt public ». Dès lors, il y avait eu à cet égard violation de l'article 10 de la CEDH.

Quant à la question concernant la réception de renseignements de l'étranger, la Cour énonce les principes suivants.

« Dès la réception des éléments interceptés, l'État destinataire doit avoir mis en place des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction. Les garanties en question, qui ont d'abord été

énoncées par la Cour dans sa jurisprudence relative à l'interception de communications par les États contractants, s'appliquent également à la réception, par un État contractant, d'éléments interceptés demandés à un service de renseignement étranger. Dès lors que les États ne sont pas toujours en mesure de savoir si des éléments reçus de services de renseignement étrangers sont le produit d'une interception, la Cour considère que les mêmes règles doivent s'appliquer à l'ensemble des éléments reçus de services de renseignement étrangers qui pourraient être le produit d'une interception » (par. 498).
Dans le cas d'espèce, qui concernait l'accord entre le Royaume-Uni et les États-Unis en matière de renseignement relatifs aux communications, la Cour considère constate que le régime de demande et de réception de renseignements émanant d'États non contractants avait une base claire en droit interne et qu'à la suite des modifications apportées au code de communication en matière d'interception de communications, ce droit était suffisamment accessible et poursuivait à n'en pas douter les buts légitimes de protection de la sécurité nationale, de défense de l'ordre et de prévention des infractions pénales, et de protection des droits et libertés d'autrui. Quant à la prévisibilité et la nécessité du régime de partage de renseignements la Cour estime que
« Le droit interne posait des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités étaient habilitées à demander des éléments interceptés à un État étranger » (par. 504).
Après un examen détaillé des conditions et garanties prévues par la loi britannique la Cour estime que les garanties mises en place au Royaume-Uni pour l'examen des données de contenu et des données de communication obtenues auprès de services de renseignement alliés, ainsi que pour l'utilisation, la conservation, la transmission à des tiers, l'effacement et la destruction de ces données étaient adéquates. De ce fait, le régime de demande et de réception d'éléments interceptés était compatible avec l'article 8 de la CEDH.

3. Bref commentaire

7. Il est hors de doute que l'arrêt *Big Brother Watch* atteint, par la nature des situations qu'il aborde et le contexte extrêmement délicat qui l'entoure, un niveau tel où le droit et la politique, qui plus est dans la sphère internationale, se recoupent inévitablement et s'entrecroisent parfois dangereusement. Tout cela semble justifier le caractère didactique et pédagogique affiché et affirmé d'un arrêt qui détaille opiniâtrement les différentes facettes d'un argumentaire d'une singulière densité. L'examen pointilleux des allégations et des prises de position des requérants et du gouvernement illustre la volonté de la Cour de traiter sans détours et esquives les aspects du contentieux qui peuvent inquiéter et fâcher à la fois, car ils frappent au cœur le réduit ultime où s'exerce une souveraineté étatique quasi intouchable, mais en fait pas tout-à-fait sans limites.
Si l'on examine de façon détaillée l'argumentaire et les considérations de l'arrêt, ce qui frappe est le sérieux méthodique qui étaye la liste des différents points traités. Sérieux méthodique, mais en fait un tantinet exagéré. Il en résulte une lecture parfois malaisée : le lecteur s'y perd dans des détails que l'on aurait pu regrouper en tête de chapitre sans alourdir, au fond, un raisonnement dont la justesse est plus qu'évidente.
On doit relever aussi que l'arrêt confirme une tendance qui s'insère dans le cadre de la répartition des compétences, nationales et supranationales, souhaitée par les Etats Parties à la CEDH et inscrite désormais clairement dans le Préambule du texte conventionnel. Cette répartition doit respecter et le principe de subsidiarité et celui de la marge d'appréciation

réservée aux Etats. Le présent arrêt en est une illustration convaincante dans la mesure où la Cour ménage ouvertement aux Etats une large marge d'appréciation concernant le bien-fondé des mesures telles l'interception en masse des communications, la réception d'éléments interceptés obtenus auprès de gouvernements et de services de renseignements étrangers, l'obtention de données de communication auprès des fournisseurs de services de communication. Il s'ensuit que la conformité avec les exigences de la CEDH porte sur le contrôle effectif de l'ensemble desdites mesures par une autorité indépendante, de préférence par un juge, sur la base de dispositions de loi qui encadrent des pouvoirs étatiques étendus et potentiellement réducteurs des libertés fondamentales. Un maillon de plus vers une conception, au niveau européen, qui fait de la « procéduralisation » des droits fondamentaux la pierre angulaire de la répartition des compétences entre la Cour de Strasbourg et les autorités nationales.

MICHELE DE SALVIA