FAQ sur l'arrêt *Big Brother Watch et autres c. Royaume-Uni*[1]

Ce document est un outil destiné à la presse, publié dans le cadre du prononcé de l'arrêt susmentionné. Il ne lie pas la Cour.

Est-ce la première fois que la Cour européenne des droits de l'homme examine des dispositions relatives à la surveillance secrète ?

La Cour européenne des droits de l'homme a traité cette question dans de nombreuses affaires, remontant au moins à 1978 (Klass c. Allemagne). Ces affaires portaient sur l'interception de communications, la collecte de données de communication, la surveillance de personnes par GPS et l'enregistrement de conversations.

L'affaire *Big Brother Watch et autres* marque-t-elle une nouvelle étape dans la jurisprudence de la Cour ?

Dans cette affaire, la Cour examine trois différents types de surveillance : l'interception massive de communications, le partage de renseignements, et l'obtention de données de communication auprès de fournisseurs de services de communication.

Ce n'est pas la première fois que la Cour se penche sur l'interception massive. Tout récemment, en juin 2018, elle a conclu que la législation et la pratique suédoises dans le domaine du renseignement électromagnétique n'emportaient pas violation de la Convention européenne des droits de l'homme (Centrum För Rättvisa c. Suède). Elle a considéré notamment que le système suédois offrait des garanties adéquates et suffisantes contre l'arbitraire et le risque d'abus. Il y a une dizaine d'années, elle s'était intéressée dans l'affaire Weber et Saravia c. Allemagne à des dispositions similaires de la loi allemande G10, et dans Liberty c. Royaume-Uni elle avait examiné le dispositif ayant précédé le système actuel d'interception massive. L'affaire *Big Brother Watch* est toutefois la première affaire dans laquelle la Cour étudie spécifiquement la portée de l'atteinte à la vie privée d'une personne qui est susceptible de résulter de l'interception et de l'examen de données de communication (par opposition au contenu de communications).

La question de l'obtention de communications auprès de fournisseurs de services de communication a également été examinée dans de précédents arrêts, notamment le récent arrêt Ben Faiza c. France.

En revanche, le partage de renseignements n'a pas encore été traité dans un arrêt de la Cour. En l'espèce, la Cour se penche pour la première fois sur la manière dont les autorités demandent et reçoivent des renseignements d'origine électromagnétique de la part d'États étrangers.

Enfin, dans l'affaire *Big Brother Watch* la Cour déclare expressément que la Commission des pouvoirs d'enquête, l'organe qui au Royaume-Uni est spécialement chargé d'examiner les plaintes pour surveillance secrète, offre à présent un recours dont les requérants doivent se prévaloir aux fins de l'épuisement des voies de recours internes et de l'examen de recevabilité. Cela vaut que le grief ait un caractère spécifique ou qu'il s'agisse d'une plainte générale sur les systèmes de surveillance. Dans Kennedy c. Royaume-Uni (2010), la Cour avait déjà exprimé des doutes sur le

[1] Voir communiqué de presse.

point de savoir si la CPE pouvait offrir un recours effectif relativement à un grief touchant au respect général de la Convention par le système britannique de surveillance secrète.

Le fait que la Cour constate dans cette affaire plusieurs violations de la Convention signifie-t-il que le Royaume-Uni doit réformer son système de surveillance massive des communications et son système d'obtention de données auprès de fournisseurs de services de communication ?

Le Royaume-Uni a actualisé ses dispositions en matière de surveillance dans le cadre d'une nouvelle législation, la loi de 2016 sur les pouvoirs d'enquête, qui n'est pas encore entrée en vigueur dans son intégralité. Dans son arrêt, la Cour n'examine pas cette nouvelle législation.

N'est-il pas important pour les États de pouvoir recourir à la surveillance secrète dans le cadre de la lutte contre le terrorisme ?

La Cour a expressément reconnu la gravité des menaces qui pèsent actuellement sur de nombreux État contractants, notamment le fléau du terrorisme international et d'autres crimes tels que le trafic de stupéfiants, la traite d'êtres humains, l'exploitation sexuelle d'enfants et la cybercriminalité. Elle a également reconnu que les avancées technologiques permettaient plus facilement aux terroristes et aux criminels de ne pas se faire repérer sur Internet. Elle a dit en conséquence que les États devaient jouir d'une ample marge d'appréciation pour choisir le meilleur moyen de protéger la sécurité nationale. Un État peut donc utiliser un système d'interception massive s'il l'estime nécessaire dans l'intérêt de la sécurité nationale.

Cela dit, la Cour ne saurait ignorer le fait que les systèmes de surveillance peuvent donner lieu à des abus, avec de graves conséquences pour la vie privée des individus. Pour réduire au minimum ce risque, la Cour a déjà eu l'occasion de définir six garanties minimales que tout système d'interception doit comporter.

Ces garanties veulent que le droit interne indique clairement les éléments suivants : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles de voir intercepter leurs communications, la limite à la durée de l'interception, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des données interceptées. Dans l'affaire Roman Zakharov c. Russie, pour déterminer si la législation litigieuse emportait violation de l'article 8, la Cour a également pris en compte les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne.

Cet arrêt est-il définitif ?

Une fois qu'un arrêt de chambre a été prononcé, les parties peuvent demander le renvoi de l'affaire devant la Grande Chambre. De telles demandes sont acceptées à titre exceptionnel. Un collège de juges de la Grande Chambre décide s'il y a lieu ou non de renvoyer l'affaire devant la Grande Chambre pour un nouvel examen.

Quelles sont les conséquences de cet arrêt pour les autres États membres ?

La Cour se penche au cas par cas sur les requêtes dont elle est saisie. Néanmoins, les autres États membres peuvent, le cas échéant, tirer des conséquences d'un arrêt rendu par la Cour de manière à

éviter que des violations similaires de la Convention européenne ne soient constatées à leur encontre.

Y a-t-il des affaires similaires pendantes ?

L'affaire 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) concerne des requêtes introduites par des avocats et des journalistes, ainsi que par des personnes morales en lien avec ces professions, au sujet de la loi française du 24 juillet 2015 relative au renseignement, qui porte sur les mesures de surveillance par des moyens électroniques. Les requêtes ont été communiquées au gouvernement français le 26 avril 2017.

La requête *Tretter et autres c. Autriche* (n^{o} 3599/10), communiquée au gouvernement autrichien le 6 mai 2013, concerne les modifications apportées en 2008 à la loi sur les pouvoirs de police, qui ont étendu les pouvoirs de collecte et de traitement des données personnelles conférés aux autorités de police.

La requête *Breyer c. Allemagne* (n^{o} 50001/12), communiquée au gouvernement allemand le 21 mars 2016, porte sur l'obligation légale pour les opérateurs de télécommunications de conserver les données personnelles de tous leurs clients.

Pour plus d'informations, voir la fiche thématique de la Cour sur la surveillance de masse.