CourEDH. Grande Chambre, 25.05.2021, Affaire Big Brother Watch et autres c. Royaume-Uni, requêtes nos. 58170/13, 62322/14 et 24960/15

L'interception massive de télécommunications et l'acquisition de données secondaires de communication (qui, où et quand) par les services de renseignement ne sont compatibles avec le droit à la vie privée (art. 8 CEDH) que si un cadre légal suffisamment strict les encadre. Des garanties procédurales de bout en bout doivent être mises en place. Parmi d'autres exigences, celles-ci doivent au moins comprendre l'autorisation préalable de la surveillance par une autorité indépendante (judiciaire ou non) et une voie de recours effective a posteriori, ouverte à toutes les personnes ayant (potentiellement) fait l'objet d'une surveillance.

Faits

À la suite des révélations d'Edward Snowden, plusieurs personnes physiques et morales contestent la conformité de la surveillance électronique déployée par les services secrets du Royaume-Uni au droit à la vie privée garanti par la CEDH (art. 8 CEDH).

Après avoir épuisé les voies de droit nationales, les requérants ont agi devant la Cour européenne des droits de l'homme. L'affaire a fait l'objet d'une première décision par la Chambre (CourEDH, 13.09.2018, Affaire Big Brother Watch et autres c. Royaume-Uni, requêtes nos. 58170/13, 62322/14 et 24960/15, résumé in: LawInside.ch/702, LawInside.ch/707, et LawInside.ch/725), puis d'une demande de renvoi devant la Grande Chambre.

Dans ce contexte, la CourEDH a examiné la conventionnalité de trois types de surveillance: (I) l'interception massive de communications ; (II) l'obtention de données de communications auprès de fournisseurs de télécoms ; et (III) le partage de renseignements avec les services secrets étrangers.

Le présent résumé s'attache à l'arrêt de la Grande Chambre, en tant qu'il traite des deux premiers types de surveillance.

L'interception massive de communications consiste à intercepter un nombre indéterminé de

communications pendant leur transmission (p. ex. l'ensemble des communications transmises par un certain câble ou un certain prestataire de télécoms). Un algorithme sélectionne ensuite selon des critères prédéfinis (les sélecteurs) les communications à conserver. Une partie des communications interceptées est ainsi supprimée automatiquement et presque en temps réel. Le système génère enfin un index des communications conservées, que les services de renseignements peuvent dès lors consulter.

Les données secondaires de communications permettent de déterminer quels utilisateurs ont communiqué, ainsi que le lieu et le moment des communications (qui, où et quand), à l'exclusion du contenu de ces communications.

La Chambre retient que l'interception massive de communication et l'obtention de données secondaires par les services de renseignements britanniques viole l'art. 8 CEDH. Par manque de densité normative, le régime britannique relatif à l'interception massive de communication ne satisferait en effet pas à l'exigence de légalité. La base légale nationale pour l'obtention de données de communication ne serait pas non plus valide, dès lors qu'elle viole les exigences du droit (supérieur) de l'UE, dont le Royaume-Uni était alors membre. En outre, la procédure mise en place ne garantirait pas la proportionnalité de la surveillance. Cela étant, la Chambre n'a pas suivi les recourants sur tous les points. En particulier, elle a considéré qu'un contrôle indépendant préalable de la mesure de surveillance n'était pas indispensable, renonçant ainsi à une exigence formelle posée de longue date par la jurisprudence de la CourEDH (CourEDH, 13.09.2018, Affaire Big Brother Watch et autres c. Royaume-Uni, requêtes nos. 58170/13, 62322/14 et 24960/15, résumé in: LawInside.ch/702, LawInside.ch/707, et LawInside.ch/725).

La Grande Chambre accepte ensuite de se saisir de l'affaire. Elle est ainsi appelée à préciser la jurisprudence de la CourEDH quant à la compatibilité de la surveillance massive des télécommunications avec le droit à la vie privée (Art. 8 CEDH).

Droit

À titre liminaire, la Grande Chambre souligne s'être déjà penchée sur l'interception massive de communications (cf. affaire Weber et Saravia c. Allemagne, requête no. 54934/00,

29.06.2006 ; et affaire Liberty et autres c. Royaume-Uni, requête no. 58243/00, 01.07.2008). Cela étant, au regard des progrès technologiques intervenus depuis ces décisions, la surveillance concerne une quantité de données bien plus grande que par le passé (« on vit de plus en plus en ligne«), et les moyens d'analyse de ces données ont été démultipliés. Il est donc nécessaire de développer la jurisprudence en la matière.

L'art. 8 CEDH garantit le droit au respect de la vie privée. Toute ingérence dans l'exercice de ce droit doit (1) avoir pour but la sauvegarde d'un intérêt légitime visé à l'art. 8 al. 2 CEDH, en particulier la sécurité nationale et la sécurité publique, (2) être prévue par la loi, et (3) s'avérer nécessaire dans une société démocratique (proportionnalité) (art. 8 al. 2 CEDH).

En l'espèce, les recourants ne contestent pas qu'au Royaume-Uni, l'interception massive de communications et l'obtention des données de communication vise à préserver des intérêts légitimes (notamment la sécurité nationale). L'examen de la Grande Chambre porte donc sur l'exigence de légalité et de proportionnalité.

Jusqu'ici, la jurisprudence (arrêts Weber et Liberty précités) énonçait un certain nombre de paramètres minimaux que la loi devait définir, y compris la nature des infractions susceptibles de donner lieu à un mandat d'interception et la définition des catégories de personnes susceptibles d'être surveillées. Or, cette approche ne tient pas compte des différences fondamentales entre la surveillance de masse et la surveillance ciblée, notamment s'agissant de leur nature et de leur échelle. En effet, l'interception massive de communications affecte par définition de larges pans de la population plutôt que des catégories de personnes spécifiques, ceci sans que des soupçons d'infractions pèsent sur la plupart des personnes touchées.

Partant, la Grande Chambre retient que pour admettre la légalité d'un système d'interception massive, elle s'attachera désormais à un nombre plus large de critères à définir dans la loi. Les garanties procédurales figurent de façon proéminente dans la nouvelle liste de critères. Des garanties de bout en bout doivent exister, afin d'encadrer chaque étape de la surveillance. Elles sont essentielles non seulement sous l'angle de la légalité, mais aussi afin d'assurer la proportionnalité de l'atteinte à la vie privée à chaque

étape (interception, conservation sur la base des sélecteurs, puis éventuelle consultation par les services secrets nationaux).

La Grande Chambre considère que l'autorisation préalable de la surveillance par une autorité indépendante est indispensable. L'autorisation d'un organe non judiciaire peut suffire, pour autant que celui-ci satisfasse à l'exigence d'indépendance. En outre, l'État doit établir une voie de droit effective permettant un contrôle *a posteriori* de l'interception de masse. La notification de l'interception à la personne concernée n'est pas indispensable ; il suffit que toute personne soupçonnant l'interception de ses communications par les services secrets puisse s'adresser à une autorité indépendante.

L'acquisition des données secondaires de communication n'est pas nécessairement moins intrusive que l'interception du contenu des communications. Dès lors, les garanties susvisées doivent en principe également encadrer l'obtention de données secondaires. Cela étant, un régime légal propre à l'acquisition des données secondaires est concevable, pour autant qu'il prévoie des garde-fous suffisants.

Appliquant ces critères au cas d'espèce, la Grande Chambre considère que le système de surveillance britannique fait l'objet d'une supervision effective par une autorité administrative indépendante, l'*Investigatory Powers Commissioner's Office*, et prévoit un recours juridictionnel solide auprès de l'*Investigatory Powers Tribunal*, ouvert à toute personne qui soupçonne l'interception de ses communications.

Cela étant, le régime britannique présente des lacunes fondamentales, en particulier l'absence d'autorisation par une autorité indépendante en amont. En effet, le ministre compétent, et non une autorité indépendante, est compétent pour autoriser l'interception de masse. Le degré de contrôle exercé en amont est au demeurant insuffisant. En particulier, le mandat n'encadre aucunement la définition des sélecteurs pour la conservation de données, qui est laissée à l'appréciation des services de renseignement.

Dans ces circonstances, les garanties de bout en bout mises en place par le Royaume-Uni sont insuffisantes ; elles ne permettent pas d'assurer la légalité et la proportionnalité de la surveillance. Partant, l'interception massive de communications et l'acquisition de données

secondaires de communication par les services secrets britannique viole le droit à la vie privée (art. 8 CEDH).

Note

La décision de la Grande Chambre ne change pas l'issue de la cause, la Chambre ayant déjà retenu une violation de l'art. 8 CEDH. Cela étant, elle constitue un important développement jurisprudentiel, dans la mesure où elle définit des exigences particulières pour un système de surveillance de masse (interception du contenu des communications et obtention des données secondaires).

En particulier, renversant la décision de la Chambre, la Grande Chambre rétablit l'exigence systématique d'un contrôle indépendant préalable. La renonciation de la Chambre à exiger un contrôle indépendant *ex ante* était à notre sens difficilement compréhensible, dans la mesure où elle relevait elle-même la compatibilité d'un tel contrôle avec le système de l'interception massive (CourEDH, 13.09.2018, Affaire Big Brother Watch et autres c. Royaume-Uni, requêtes nos. 58170/13, 62322/14 et 24960/15, par. 318). La mise en place de garde-fous appropriés, notamment sous l'angle procédural, est essentielle au regard de la tendance actuelle à la généralisation de la surveillance étatique. Nous nous réjouissons donc de la confirmation de cette importante garantie formelle.

L'auteure du présent résumé avait commenté l'arrêt de la chambre: Émilie Jacot-Guillarmod, La surveillance des télécommunications, in : Jusletter, September 2018, 2-12.

Proposition de citation : Emilie Jacot-Guillarmod, La surveillance des télécommunications par les services secrets: Arrêt de la Grande Chambre (CourEdH, Big Brother Watch) (I/II), in: https://lawinside.ch/1063/