CourEDH, 13.09.2018, Affaire Big Brother Watch et autres c. Royaume-Uni, requêtes nos. 58170/13, 62322/14 et 24960/15

Les États parties peuvent recevoir d'États tiers le produit d'interceptions de communications sans violer le droit à la vie privée (art. 8 CEDH), à certaines conditions. Il faut en particulier que cette mesure repose sur une base légale qui détermine clairement les conditions pour une requête de partage, la procédure pour l'examen et la conservation des données interceptées, les précautions à prendre en cas de partage ultérieur desdites données, ainsi que les modalités de suppression de ces données.

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 agissent devant la Cour européenne des droits de l'homme.

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

Le présent résumé s'attache au deuxième de ces trois types de surveillance.

Lorsqu'ils ne sont pas en mesure d'obtenir directement les informations correspondantes, les services secrets britanniques peuvent demander aux autorités étrangères d'intercepter certaines communications ou de leur remettre certaines données interceptées. La CourEDH examine si la remise de renseignements aux services secrets britanniques par la NSA selon ces modalités viole le droit à la privée (art. 8 CEDH).

Droit

L'art. 8 CEDH garantit le droit au respect de la vie privée. À titre liminaire, la CourEDH

examine la nature de l'ingérence litigieuse dans l'exercice de ce droit. L'interception en tant que telle ne relève pas du champ d'application territorial de la CEDH, puisqu'elle intervient hors du Royaume-Uni et sous le seul contrôle de la NSA, une autorité d'un État qui n'est pas partie à la CEDH. Partant, le contrôle de la CourEDH se limite à la conformité à l'art. 8 CEDH de l'obtention des données concernées et de leur traitement ultérieur par les autorités britanniques.

À teneur de l'art. 8 al. 2 CEDH, ces mesures doivent (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)

Selon le droit anglais, le partage de renseignements n'est permis qu'en vue de la sauvegarde de la sécurité nationale ou de la lutte contre de graves infractions, soit des intérêts légitimes au sens de l'art. 8 al. 2 CEDH.

En vertu du principe de légalité, l'ingérence doit avoir une base légale accessible à la personne concernée et suffisamment prévisible dans ses effets. Sous l'angle de la prévisibilité, par analogie avec sa jurisprudence en matière d'interception massive de communications, la CourEDH retient que la loi doit prévoir au moins les éléments suivants en cas de partage de communications interceptées: la procédure pour l'examen et la conservation des données interceptées, les précautions à prendre en cas de partage ultérieur desdites données, et les circonstances dans lesquelles une suppression de ces données s'impose. En outre, la loi doit préciser à quelles conditions les services de renseignements peuvent demander à un État tiers de leur communiquer des données interceptées.

La loi britannique traite les éléments susvisés de façon suffisamment claire. En particulier, les services secrets ne peuvent solliciter la communication de données par un État tiers que si un mandat d'interception national pour les mêmes données existe déjà ou, exceptionnellement (par exemple lorsqu'une interception sur sol britannique apparaît en tout état irréalisable), si une autorisation ad hoc a été rendue. De plus, les mêmes règles s'appliquent au traitement de données reçues d'États tiers qu'au traitement de données

interceptées directement par les services secrets britanniques. Ceci comprend notamment le *Data Protection Act* anglais.

Dans son examen de la proportionnalité d'un système de surveillance, la CourEDH attache une importance particulière à l'effectivité des cautèles procédurales prévues par la loi. Au Royaume-Uni, des garanties procédurales similaires s'appliquent à l'interception de communications sur sol national et à la requête de renseignements auprès d'une autorité étrangère: comme évoqué précédemment, une telle requête de renseignements doit notamment reposer sur un mandat d'interception domestique ou sur une autorisation ad hoc du Secrétaire d'État (*Secretary of State*). Un commissaire indépendant, l'*Interception of Communications Commissioner* doit être informé de l'autorisation ad hoc de la demande de renseignements. Ce commissaire supervise également les accords d'échanges de renseignements entre les services secrets britanniques et étrangers. Enfin, un tribunal indépendant, l'*Investigatory Powers Tribunal* (IPT), est compétent pour examiner les doléances de toute personne dont les communications auraient pu faire l'objet d'un tel transfert de renseignements. De façon générale, ces cautèles procédurales apparaissent propres à empêcher les autorités de contourner leurs obligations en vertu de la CEDH en demandant à des autorités tierces d'obtenir des informations à leur place et à garantir la proportionnalité de l'ingérence correspondante dans d'exercice du droit à la vie privée.

À la lumière de ce qui précède, la CourEDH retient que le système d'échange de renseignements entre les services secrets britanniques et la NSA ne viole pas le droit à la vie privée (art. 8 CEDH).

Note

La première partie de cet arrêt, relative à l'interception massive de communications, est résumée *in* LawInside.ch/702.

Cet arrêt n'est pas définitif au moment de la publication du présent résumé. Une demande de renvoi devant la Grande Chambre est pendante.

C'est la première fois que la CourEDH examine un système de partage de renseignements

entre les services secrets de plusieurs États.

Il sied de relever que cet arrêt examine uniquement la conventionnalité de la réception (*inbound*) de renseignements par les autorités d'un État partie à la CEDH. Il ne traite pas de la remise d'informations (*outbound*) à des autorités tierces.

Les exigences formulées ici par la CourEDH en matière de prévisibilité reposent largement sur la jurisprudence existante en matière d'interception massive, adaptée aux circonstances particulières de la réception de renseignements. Selon la jurisprudence en matière d'interception massive (cf. p. ex. 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, et première partie du présent arrêt), les aspects suivants au moins doivent être prévus par la loi: (1) la nature des infractions susceptibles de donner lieu à un mandat d'interception, (2) la définition des catégories de personnes susceptibles d'être mises sur écoute, (3) la fixation d'une limite à la durée de l'exécution de la mesure, (4) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, (5) les précautions à prendre pour la communication des données à d'autres parties, et (6) les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

À notre sens, la cohérence voudrait que la légalité de la remise d'informations à des autorités tierces réponde à des critères similaires. En particulier, dès lors que l'État partie effectuerait l'interception, il nous semble que la loi devrait prévoir les points (1) à (3) susvisés également lorsque l'interception intervient à la demande d'un État tiers. En outre, il nous semble que l'État tiers devrait présenter certaines garanties quant à l'utilisation, la communication ultérieure et la destruction des renseignements communiqués (points (4) à (6) ci-dessus). Dans ce contexte, nous relevons qu'en cas de réception de renseignements (*inbound*), l'arrêt résumé ici prend en compte la législation applicable en matière de protection des données. Selon le même raisonnement, la possibilité de communiquer des renseignements (*outbound*) devrait à notre sens prendre en compte les règles de protection des données applicables dans l'État de destination et pourrait s'intéresser à la conformité de ces dernières aux instruments pertinents du Conseil de l'Europe, notamment la

Convention 108.

Proposition de citation : EMILIE JACOT-GUILLARMOD, La surveillance des télécommunications par les services secrets (CourEDH) (II/III), in: https://lawinside.ch/707/