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

En tant que telle, l'interception massive de communications n'excède pas la marge d'appréciation laissée aux Etats pour préserver leur sécurité nationale. Il n'est pas indispensable que la mise en œuvre d'une telle surveillance face l'objet d'un contrôle ex ante *par une autorité indépendante. Les bases légales et la procédure nationales doivent cependant présenter une densité normative suffisante et garantir la proportionnalité.*

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 premier de ces trois 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 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.

La CourEDH doit déterminer si ce système de surveillance viole le droit à la privée (art. 8

CEDH).

Droit

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).

In casu, les recourants ne contestent pas que selon les dispositions nationales applicables, l'interception massive de communications ne peut intervenir qu'en vue de la sauvegarde de la sécurité nationale ou de la lutte contre de graves infractions. Les buts poursuivis par ce type de surveillance au Royaume-Uni correspondent ainsi à des intérêts légitimes au sens de l'art. 8 al. 2 CEDH.

En vertu du principe de légalité, la loi topique doit être accessible à la personne concernée. Cela étant, par nature, tous les détails d'un régime de surveillance secrète ne peuvent être rendus accessibles au public. Partant, il s'agit de s'assurer que les bases légales accessibles au public assurent un degré de prévisibilité suffisant et respectent le principe de la proportionnalité.

À teneur de jurisprudence, pour que son application soit suffisamment prévisible, la loi doit nécessairement prévoir certains éléments, en particulier les catégories de personnes dont les communications peuvent être interceptées, la procédure pour l'examen, l'usage et la conservation des données issues de l'interception, et les cas dans lesquels les données interceptées doivent être supprimées. La CourEDH relève qu'un régime d'interception massive permettra nécessairement l'interception de larges catégories de communications. Ceci ne signifie pas *per se* qu'une telle forme de surveillance est incompatible avec les exigences de prévisibilité et de proportionnalité. Une sélection plus rigoureuse des communications conservées devra en revanche impérativement intervenir dans un second temps et faire l'objet de garanties législatives et procédurales suffisantes.

S'agissant de la proportionnalité, la CourEDH reconnaît aux Etats une certaine marge d'appréciation quant aux moyens à déployer pour protéger leur sécurité nationale. En tant que telle, l'interception massive de communications n'excède pas cette marge d'appréciation. Dans ce contexte, la CourEDH examine si les garanties procédurales mises en place aux différentes étapes du processus de surveillance suffisent à prévenir les abus. Les exigences de légalité et de proportionnalité se rejoignent ainsi dans une certaine mesure.

Contrairement à ce que soutiennent les recourants, le simple fait que l'interception massive ne requiert pas d'autorisation judiciaire ne viole pas l'art. 8 CEDH. Si la supervision par une autorité judiciaire est en principe souhaitable, elle n'est pas strictement nécessaire. Dans le système anglais, le Secrétaire d'État (*Secretary of State*) autorise l'interception massive, sous la surveillance d'un commissaire indépendant, l'*Interception of Communications Commissioner*. Par ailleurs, toute personne qui pense avoir fait l'objet d'une surveillance secrète peut demander à un tribunal indépendant, l'*Investigatory Powers Tribunal*, d'examiner si une telle surveillance est intervenue et respectait la loi. De façon générale, ces cautèles procédurales apparaissent propres à garantir la proportionnalité de la surveillance et à prévenir des abus.

Toutefois, les juges de Strasbourg relèvent que la loi anglaise ne définit pas précisément quels relais de communication peuvent dans un premier temps faire l'objet d'interceptions, ni selon quels critères de sélection les communications doivent être supprimées ou sauvegardées dans un second temps. L'autorisation du Secrétaire d'Etat ne définit pas non plus ces éléments, qui ne peuvent dès lors faire l'objet d'un contrôle effectif ni par l'*Interception of Communications Commissioner*, ni par l'*Investigatory Powers Tribunal* (« IPT »).

Partant, la CourEDH retient que par manque de densité normative, le régime britannique ne satisfait pas à l'exigence de légalité. En outre, la procédure mise en place ne garantit pas la proportionnalité de la surveillance. La CourEDH admet dès lors la requête sur ce point et constate que le système d'interception massive de communication mis en place par le Royaume-Uni viole l'art. 8 CEDH.

Note

La deuxième partie de cet arrêt, relative à la réception (*inbound*) du produit d'interceptions de communications, est résumée *in* LawInside.ch/707.

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

Ce n'est pas la première fois que la CourEDH se penche sur l'interception massive de communications. Cet arrêt constitue pour l'essentiel la confirmation de jurisprudences préalables (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). Les recourants faisaient valoir qu'au regard de l'évolution technologique et des modes de communication, l'interception massive représentait une ingérence beaucoup plus grave aujourd'hui que lors du développement de ces exigences jurisprudentielles, il y a plus de dix ans. Précisons que dans le seul autre arrêt récent de la CourEDH en la matière (Affaire Centrum för Rättvisa c. Suède, 19 juin 2018, requête no. 35252/08, non définitif), l'interception faisait l'objet d'un contrôle judiciaire préalable. La CourEDH n'a toutefois pas suivi les recourants et a en particulier confirmé que le contrôle *ex ante* par une autorité indépendante n'était pas strictement nécessaire.

Les juges de Strasbourg ne sont pas unanimes sur ce point. Dans leur *partly concurring, partly dissenting opinion,* les juges Koskelo et Turkovic se prononcent en faveur de l'exigence systématique d'un contrôle indépendant *ex ante* de l'interception massive.

A priori, les exigences de la CJUE au regard de la Charte des droits fondamentaux de l'UE apparaissent plus strictes sur ce point. Selon les standards développés par la CJUE (CJUE, Digital Rights Ireland, C-293/12 et C-594/12, 08.04.2014; et Tele2 Sverige AB, C-203/15 et C-698/15, 17.07.2015) pour l'obtention de données de communications auprès de fournisseurs de télécoms, l'accès aux données par les autorités doit être soumis à l'autorisation préalable d'une instance judiciaire ou administrative indépendante. Cela étant, la CJUE n'a pas encore tranché si un tel contrôle indépendant *ex ante* est indispensable également pour accéder aux données obtenues par l'interception massive.

Cette question fait l'objet d'une question préjudicielle de l'IPT actuellement pendante devant la CJUE (Cas C-623/17, question préjudicielle du 31 octobre 2017).

Proposition de citation : Emilie Jacot-Guillarmod, La surveillance des télécommunications par les services secrets (CourEDH) (I/III), in: https://lawinside.ch/702/