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

La base légale nationale permettant aux services secrets britanniques d'obtenir des données de communications viole le droit de l'UE. Or, le droit communautaire prévaut sur le droit national en cas de conflit. Le régime de surveillance anglais ne satisfait dès lors pas à l'exigence de légalité et viole de ce fait le droit à la vie privée (art. 8 CEDH).

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 secondaires de communications auprès de fournisseurs de télécoms.

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

Les données secondaires de communications permettent de déterminer quels utilisateurs ont communiqués, ainsi que le lieu et le moment des communications (qui, où et quand), à l'exclusion du contenu de ces communications. La CourEDH examine si l'obtention de telles données par les services secrets britanniques viole le droit à la privée (art. 8 CEDH).

Droit

L'art. 8 CEDH garantit le droit au respect de la vie privée. À teneur de l'art. 8 al. 2 CEDH, une ingérence dans l'exercice de ce droit est admissible si elle (1) est prévue par la loi, (2) a pour but la sauvegarde d'un intérêt légitime visé à l'art. 8 al. 2 CEDH, en particulier la prévention des infractions pénales, la sécurité nationale et la sécurité publique, et (3)

s'avère nécessaire dans une société démocratique (proportionnalité).

À titre liminaire, la CourEDH relève que sous l'angle du droit de l'Union européenne, la question de l'accès par les autorités nationales aux données secondaires de communications a fait l'objet de plusieurs arrêts de la Cour de Justice de l'Union européenne (CJUE) (CJUE, décision du 8 avril C-293/12 et C-594/12, Digital Rights Ireland, et décision du 21 décembre 2016 C-203/15 et C-698/15, Tele2 Sverige). Dans ces arrêts, la CJUE retient notamment que l'accès des autorités à de telles données doit faire l'objet d'un contrôle préalable par une autorité administrative ou judiciaire indépendante et, dans le domaine du droit pénal, être restreint à ce qui est strictement nécessaire pour lutter contre de graves infractions.

Le Royaume-Uni étant membre de l'Union européenne, l'ordre juridique de l'Union, y compris la jurisprudence de la CJUE susvisée, fait partie intégrante de son ordre juridique. En cas de conflit entre le droit national et celui de l'Union, ce dernier prévaut.

Or, la *High Court of Justice* anglaise a jugé que la base légale nationale pour l'obtention de données secondaires de communications par les services secrets du Royaume-Uni, l'*Investigatory Powers Act* (IPA), ne remplissait pas les exigences posées par la CJUE (High Court of Justice, décision 2018 EWHC 975 (Admin) du 27 avril 2018). En effet, cette loi ne soumet pas l'accès aux données à un contrôle indépendant préalable. Par ailleurs, dans le domaine du droit pénal, l'IPA ne limite pas les possibilités d'accès à la lutte contre les infractions graves.

Dans la mesure où l'IPA n'est pas conforme au droit communautaire supérieur, la CourEDH retient qu'il n'existe pas de base légale nationale valide pour l'obtention des données secondaires de communications par les services secrets britanniques.

Partant, l'ingérence n'est pas admissible au regard de l'art. 8 al. 2 CEDH.

Note

Les deux premières parties de cet arrêt, relatives à l'interception massive de communications et au partage de renseignements avec les services secrets étrangers, sont résumées in: LawInside.ch/702 et LawInside.ch/707.

Cet arrêt n'est pas définitif au moment de la publication du présent résumé. La CourEDH a accepté le 5 février 2019 une demande de renvoi devant la Grande Chambre.

Il sied de souligner que la CourEDH examine ici uniquement la légalité de l'ingérence (cf. art. 8 al. 2 CEDH 1ère condition), soit la conformité de la base légale invoquée à une source supérieure de droit domestique. Selon la perspective adoptée ici par la CourEDH, c'est le droit communautaire et non la CEDH qui exige un contrôle indépendant préalable et une limitation de la surveillance à ce qui est strictement nécessaire pour lutter contre les infractions graves. En matière d »interception massive de communications (considérants résumés in: LawInside.ch/702), l'arrêt résumé ici retient d'ailleurs qu'un contrôle indépendant préalable n'est pas indispensable au regard de l'art. 8 al. 2 CEDH. D'autres cautèles procédurales, y compris un contrôle judiciaire *a posteriori*, peuvent satisfaire aux exigences de la CEDH.

Il reste à déterminer si le présent arrêt influencera la jurisprudence de la CJUE. Jusqu'ici, la CJUE a refusé de trancher si les dispositions pertinentes de la charte des droits fondamentaux de l'Union européenne (art. 7 et 8 de la charte) conféraient une protection plus étendue que l'art. 8 CEDH, tout en précisant que son analyse s'opérait exclusivement au regard de la charte des droits fondamentaux de l'Union européenne (cf. affaire Tele2 Sverige susvisée). Si la CJUE maintient sa jurisprudence, le régime de la charte divergera de celui de la CEDH, les exigences de la charte s'avérant plus strictes que celles de la CEDH.

La conservation des données secondaires de communications par les opérateurs, qui constituait la question centrale des décisions susvisées de la CJUE, n'était pas litigieuse devant la CourEDH *in casu*. À notre connaissance, la CourEDH ne s'est jamais prononcée sur la conventionnalité de la conservation des données secondaires de communication par les opérateurs. Cela étant, on peut tirer certains enseignements de la position adoptée ici par la CourEDH en matière d'interception massive: la CourEDH a en effet considéré qu'en tant que telle, l'interception de larges catégories de communications n'exclut pas la conformité de la surveillance à l'art. 8 CEDH. En outre, la CourEDH considère que par nature, l'interception de données secondaires représente une atteinte moindre au droit à la

vie privée que l'interception du contenu des communications (CourEDH, décision du 02.08.1984, requête 8691/79, Malone et al. c. Royaume Uni, confirmé dans le présent arrêt). Partant, *per se*, l'interception indiscriminée de vastes volumes de données secondaires de communication ne devrait pas violer la CEDH. Par opposition, la CJUE a jugé que la charte des droits fondamentaux de l'Union européenne s'opposait à la conservation indiscriminée de l'ensemble des données de communications pendant plusieurs mois (affaires Digital Rights Ireland et Tele2 Sverige susvisées).

En Suisse, le Tribunal fédéral a récemment examiné si l'obligation faite aux opérateurs téléphoniques de conserver durant six mois les données secondaires de communications (art. 15 al. 3 aLSCPT, actuellement art. 26 al. 5 LSCPT) était conforme au droit à la vie privée (ATF 144 I 126, résumé in: LawInside.ch/600). Il a expressément exclu la possibilité de transposer directement la jurisprudence de la CJUE susvisée au droit suisse et a retenu que le régime de la LSCPT était conforme à la CEDH, au regard des conditions strictes posées par le CPP pour l'accès aux données. À la lumière de ce qui précède, la position du Tribunal fédéral, en particulier la différenciation entre les exigences du droit communautaire (non applicables en Suisse) et celles de la CEDH (applicables en Suisse), nous paraît défendable.

Proposition de citation : EMILIE JACOT-GUILLARMOD, La surveillance des télécommunications par les services secrets (CourEDH) (III/III), in: https://lawinside.ch/725/