www.jusletter.ch

Emilie Jacot-Guillarmod

La surveillance des télécommunications (art. 8 CEDH)

CourEDH, arrêt Big Brother Watch et autres c. Royaume-Uni du 13 septembre 2018

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat in einem vielbeachteten Urteil untersucht, ob die Überwachung der Telekommunikation durch den britischen Geheimdienst das Recht auf Privatleben nach Art. 8 EMRK verletzt hat. Die Autorin fasst das Urteil zusammen und prüft dessen Tragweite im Licht der früheren Rechtsprechung sowie die möglichen Auswirkungen auf gewisse noch offene Fragen, etwa zur Zulässigkeit der Aufbewahrung von Randdaten der Telekommunikation. Die Autorin stellt dieses Urteil auch in den Kontext einschlägiger Entscheide des Gerichtshofs der Europäischen Union (EuGH). (as)

Beitragsarten : Urteilsbesprechungen
Rechtsgebiete : EMRK, Menschenrechte, Datenschutz

Proposition de citation : Emilie Jacot-Guillarmod, La surveillance des télécommunications (art. 8 CEDH), in : Jusletter 17. Juni 2019

Table des matières

Introduction

[Rz 1] Les révélations d'Edward Snowden, ancien employé de la *Central Intelligence Agency* (CIA) et de la *National Security Agency* (NSA) américaines, quant aux programmes de surveillance de masse mis en œuvre par divers pays occidentaux ont fait couler beaucoup d'encre au cours des dernières années.

[Rz 2] Elles ont aussi donné lieu à plusieurs procédures judiciaires, notamment au Royaume-Uni, des groupes issus de la société civile et personnes privées considérant la surveillance exercée par les services secrets britanniques comme une violation de leur droit fondamental à la vie privée. Après avoir épuisé les voies de recours nationales, certains des requérants ont porté le cas devant la CourEDH.

[Rz 3] Dans *Big Brother Watch et autres c. Royaume-Uni* du 13 septembre 2018[1], un arrêt-fleuve de plus de 200 pages (y compris deux opinions partiellement dissidentes et partiellement concordantes), la CourEDH s'est ainsi penchée sur le système de surveillance généralisée des télécommunications établi par un Etat moderne. Plus précisément, la CourEDH a analysé la conformité à l'art. 8 de la Convention européenne des droits de l'homme (CEDH) de trois régimes de surveillance :

1. l'interception massive de communications ;
2. le partage de renseignements avec les services secrets étrangers ; et
3. l'obtention de données de communications auprès de fournisseurs de télécoms.

[Rz 4] La présente contribution résume et commente[2] de façon concise l'analyse de la CourEDH quant à la conformité des trois types de surveillance susvisés au droit à la vie privée et familiale garanti par l'art. 8 CEDH. A teneur de l'art. 8 al. 2 CEDH, l'ingérence d'une autorité publique

1 Ci-après « arrêt *Big Brother Watch* ».

2 Un résumé de l'arrêt *Big Brother Watch* et certains des commentaires que nous formulons ici figurent également in : Emilie Jacot-Guillarmod, *La surveillance des télécommunications par les services secrets (CourEDH)*, www.lawinside.ch/702/ ; www.lawinside.ch/707/ ; et http ://www.lawinside.ch/725/, dernière consultation en juin 2019).

dans l'exercice de ce droit n'est admissible que si elle (i) est prévue par la loi (légalité) ; (ii) a pour but la sauvegarde d'un intérêt légitime visé à l'art. 8 al. 2 CEDH ; et (iii) s'avère nécessaire dans une société démocratique (proportionnalité). L'existence d'intérêts légitimes au sens de l'art. 8 al. 2 CEDH n'était pas litigieuse *in casu*, dans la mesure où le système de surveillance britannique vise à préserver la sécurité nationale (notamment du terrorisme) et à lutter contre les infractions pénales. Nous nous penchons dès lors uniquement sur la légalité et la proportionnalité de la surveillance de chaque type de surveillance. Dans une brève digression, nous examinons ensuite les implications de cette jurisprudence pour la question connexe de la conservation indiscriminée de vastes volumes de données secondaires par les opérateurs de télécoms. Nous concluons par une discussion des conséquences possibles de cette jurisprudence, étant précisé que l'arrêt *Big Brother Watch* n'est pas définitif, la CourEDH ayant accepté une requête de renvoi devant la Grande Chambre[3].

I. L'interception massive de communications

a. Remarques liminaires

[Rz 5] 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 relais de télécommunications). Dans le système britannique, 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 consulter.

b. Légalité

[Rz 6] La CourEDH a déjà eu l'occasion de se pencher sur la légalité de l'interception d'un nombre indéterminé de télécommunications[4]. Sous l'angle de la légalité, la jurisprudence existante exige que la base légale de la surveillance soit accessible à la personne concernée[5]. Cela étant, dans l'arrêt *Big Brother Watch*[6], la CourEDH a relevé que par nature, tous les détails d'un régime de surveillance secrète ne peuvent être rendus accessibles au public. Partant, la Cour a examiné si les bases légales accessibles au public assuraient un degré de prévisibilité suffisant.

[Rz 7] À teneur de jurisprudence[7], pour que son application soit suffisamment prévisible, la loi doit au moins prévoir les éléments suivants :

---

3 CourEDH, Communiqué de presse du Greffier de la Cour, Décisions du collège de la Grande Chambre du 5 février 2019, 053 (2019).

4 Arrêt de la CourEDH *Liberty et autres c. Royaume-Uni* du 1er juillet 2008, 58243/00 (ci-après « arrêt *Liberty* ») ; et arrêt de la CourEDH *Weber et Saravia c. Allemagne* du 20 juin 2006, 52934/00 (ci-après « arrêt *Weber* »).

5 Cf. en particulier arrêt de la CourEDH *Liberty et autres c. Royaume-Uni* du 1er juillet 2008, 58243/00 précité, par. 59 ; arrêt de la CourEDH *Weber et Saravia c. Allemagne* du 20 juin 2006, 52934/00 précité, par. 84 ; arrêt de la CourEDH *Lambert c. France* du 24 août 1998, 88/1997/872/1084 (ci-après « arrêt *Lambert* »), par. 26 ; et arrêt *Kruslin c. France* du 24 avril 1990, 11801/85, par. 27.

6 CourEDH, arrêt *Big Brother Watch*, par. 326.

7 CourEDH, arrêt *Liberty* précité, par. 62 ; et arrêt *Weber* précité, par. 95.

1. la nature des infractions susceptibles de donner lieu à un mandat d'interception ;
2. la définition des catégories de personnes susceptibles d'être surveillées ;
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 la destruction des enregistrements s'impose.

[Rz 8] La CourEDH a confirmé cette jurisprudence *in casu*[8]. La Cour a retenu que si un régime d'interception massive permettait nécessairement l'interception de larges catégories de communications, ceci ne signifiait pas *per se* qu'une telle forme de surveillance est incompatible avec l'exigence de prévisibilité[9]. Une sélection plus rigoureuse des communications conservées devait en revanche impérativement intervenir dans un second temps[10].

[Rz 9] Or, dans le cas d'espèce, la base légale divulguée publiquement ne définissait pas précisément quels relais de communication pouvaient dans un premier temps faire l'objet d'interceptions, ni selon quels critères de sélection les communications devaient être supprimées ou sauvegardées dans un second temps[11]. Partant, en raison de son manque de densité normative, le régime britannique ne satisfaisait pas à l'exigence de légalité[12].

[Rz 10] En ce qui concerne la légalité d'un système d'interception massive, les considérants susvisés constituent essentiellement une confirmation de jurisprudence. Cela étant, c'est à notre connaissance la première fois que la Cour aborde expressément le lien entre l'accessibilité et la prévisibilité, jusqu'ici traitées comme deux exigences distinctes et cumulatives[13]. L'approche adoptée ici, soit considérer que la base légale est suffisamment accessible si les dispositions publiques assurent un degré de prévisibilité suffisant, nous paraît cohérente et apporte un éclaircissement bienvenu dans le domaine de la surveillance secrète, où certains arrangements sont typiquement gardés confidentiels.

c. Proportionnalité

[Rz 11] S'agissant de la proportionnalité, dans l'arrêt *Big Brother Watch*[14], la CourEDH a rappelé reconnaitre aux Etats une certaine marge d'appréciation quant aux moyens à déployer pour protéger leur sécurité nationale[15]. En tant que telle, l'interception massive de communications n'excédait pas cette marge d'appréciation[16]. Dans ce contexte, la Cour a examiné si les garan-

8 CourEDH, arrêt *Big Brother Watch*, par. 320.

9 CourEDH, arrêt *Big Brother Watch*, par. 338.

10 *Ibid*.

11 CourEDH, arrêt *Big Brother Watch*, par. 346 s.

12 CourEDH, arrêt *Big Brother Watch*, par. 346 s. et par. 387.

13 Dans l'arrêt *Liberty*, les requérantes faisaient déjà valoir que la loi nationale ne satisfaisait pas à l'exigence de prévisibilité, certains aspects clefs de la loi n'étant pas accessibles (CourEDH, arrêt *Liberty* précité, par. 60). La CourEDH n'a toutefois pas expressément traité la question de la relation entre ces deux exigences dans l'arrêt *Liberty*.

14 CourEDH, arrêt *Big Brother Watch*, par. 283, 308, 314 et 387.

15 En ce sens déjà, CourEDH, arrêt *Weber* précité, par. 106 ; arrêt *Lambert* précité, par. 31 ; arrêt *Camenzind c. Suisse* du 16 décembre 1997, 21353/93, par. 45 ; arrêt *Leander c. Suède* du 26 mars 1987, 9248/81, par. 59 ; arrêt *Klass et autres c. Allemagne* du 6 septembre 1978, 5029/71, par. 49 s.

16 En ce sens déjà, CourEDH, arrêt *Weber* précité, par. 137.

ties procédurales mises en place aux différentes étapes du processus de surveillance litigieux suffisaient à prévenir les abus.

[Rz 12] *In casu*, les requérants faisaient valoir que la CourEDH devait reconsidérer les exigences développées jusque-là dans sa jurisprudence quant aux cautèles procédurales nécessaires[17], au regard de l'évolution technologique et des modes de communication[18]. Ils argumentaient en particulier qu'un contrôle judiciaire indépendant avant l'autorisation de la surveillance était indispensable[19]. En effet, selon les requérants, l'interception massive représentait une ingérence beaucoup plus grave aujourd'hui que lors du développement de ces exigences, il y a plus de dix ans[20].

[Rz 13] La CourEDH n'a pas suivi les requérants sur ce point. Elle a retenu que la simple absence d'autorisation judiciaire préalable ne violait pas l'art. 8 CEDH. Si la supervision de l'interception massive par une autorité judiciaire était en principe souhaitable, elle n'était pas strictement nécessaire[21]. Cette position n'est pas nouvelle : si la CourEDH exigeait jusque-là un contrôle indépendant *ex ante*, elle admettait que le contrôle préalable par une autorité administrative indépendante pouvait suffire à garantir la proportionnalité de la mesure[22]. Dans l'arrêt *Big Brother Watch*, la Cour va cependant plus loin et renonce à exiger un quelconque contrôle indépendant préalable, qu'il soit judiciaire ou administratif[23]. La procédure nationale ne doit ainsi répondre à aucune exigence formelle, mais doit présenter dans son ensemble des cautèles suffisantes et ne pas donner lieu à des abus dans son fonctionnement effectif[24].

[Rz 14] A notre sens, la jurisprudence *Big Brother Watch* constitue un changement de paradigme : jusqu'ici, la CourEDH exigeait un contrôle indépendant *ex ante* de la proportionnalité de la surveillance, et examinait au demeurant la procédure dans son ensemble, ainsi que son fonctionnement effectif. Le contrôle indépendant préalable constituait ainsi une garantie nécessaire, mais non suffisante[25]. Dans l'arrêt *Big Brother Watch*, la Cour renverse ce raisonnement en considérant que puisque le contrôle indépendant préalable ne suffit pas à garantir la proportionnalité de la

17 Cf. notamment CourEDH, arrêts *Weber* et *Liberty* précités.

18 CourEDH, arrêt *Big Brother Watch* précité, par. 316.

19 *Ibid.*

20 *Ibid.*

21 CourEDH, arrêt *Big Brother Watch* précité, par. 318 ss. Dans le cas d'espèce, la CourEDH a retenu que les garanties procédurales mises en place par le Royaume-Uni apparaissaient généralement propres à garantir la proportionnalité de la surveillance et à prévenir des abus. En effet, dans le système anglais, l'autorisation de l'interception massive intervenait sous la surveillance d'un commissaire indépendant. Par ailleurs, toute personne qui pensait avoir fait l'objet d'une surveillance secrète disposait d'un recours effectif *a posteriori* devant un tribunal indépendant. Ce nonobstant, la CourEDH a retenu que le manque de densité normative de la loi topique (cf. section II.b ci-dessus) entravait en l'espèce le contrôle des catégories de données interceptées et empêchait ainsi les cautèles procédurales établies de fonctionner en la matière. Dans cette mesure, le système d'interception massive de communication mis en place par le Royaume-Uni violait l'art. 8 CEDH.

22 CourEDH, arrêt *Centrum för Rättvisa c. Suède* du 19 juin 2018, 35252/08 (ci-après « arrêt *Rättvisa* »), par. 153 ss ; arrêt *Szabó et Vissy c. Hungary* du 6 juin 2016, 37138/14 (ci-après « arrêt *Szabo* »), par. 77 ss ; arrêt *Roman Zakharov c. Russie* du 4 décembre 2015, 47143/06 (ci-après « arrêt *Zakharov* »), par. 258 ; arrêt *Dumitru Popescu c. Roumanie* du 26 avril 2007, 71525/01, par. 71 ; et arrêt *Weber* précité, par. 115. Il est précisé que la Cour a admis le renvoi de l'arrêt *Rättvisa* devant la Grande Chambre.

23 CourEDH, arrêt *Big Brother Watch* précité, par. 320 et 381.

24 *Ibid.*

25 Parmi d'autres, la CourEDH a ainsi notamment considéré que la procédure nationale était impropre à garantir la proportionnalité de la surveillance nonobstant un contrôle indépendant dans les cas suivants : arrêt *Mustafa Sezgin Tanrkulu c. Turquie* du 18 juillet 2017, 27473/06 ; arrêts *Szabo* et *Zakharov* précités ; et arrêt *Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie* du 28 juin 2007, 62540/00.

surveillance, il n'est pas non plus indispensable[26]. Cette conclusion ne nous paraît pas s'imposer. Au regard de la tendance actuelle à la généralisation de la surveillance étatique, cette renonciation à une importante garantie formelle pourtant compatible avec le système de l'interception massive[27] nous semble regrettable. Les juges n'étaient d'ailleurs pas unanimes à ce sujet. Dans leur opinion conjointe partiellement dissidente et partiellement concordante, les juges Koskelo et Turkovic se sont en effet prononcés en faveur de l'exigence systématique d'un contrôle indépendant *ex ante* de l'interception massive.

[Rz 15] *A priori*, les exigences de la CJUE au regard de la Charte des droits fondamentaux de l'Union européenne[28] sont plus strictes en la matière. Selon les standards développés par la CJUE pour l'obtention de données de communications auprès de fournisseurs de télécoms[29], 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* était indispensable également pour l'interception massive. Cette question fait l'objet d'une question préjudicielle de l'IPT actuellement pendante devant la CJUE[30].

II. Le partage de renseignements avec les services secrets étrangers

a. Remarques liminaires

[Rz 16] Le droit britannique permet aux services secrets de demander aux autorités étrangères d'intercepter certaines communications ou de leur remettre certaines données interceptées, lorsqu'ils ne sont pas en mesure d'obtenir directement les informations correspondantes. *In casu*, les requérants contestaient plus particulièrement la réception de renseignements fournis par la NSA.

[Rz 17] L'arrêt *Big Brother Watch* constitue le premier arrêt de la CourEDH relatif au partage de renseignements issus de la surveillance secrète.

b. Légalité

[Rz 18] A titre liminaire, la CourEDH a relevé qu'en tant que telle, l'interception ne relevait pas du champ d'application territorial de la CEDH, puisqu'elle intervenait hors du Royaume-Uni et sous le seul contrôle de la NSA, une autorité d'un Etat non partie à la CEDH[31]. Partant, la Cour a restreint son contrôle à la conformité à l'art. 8 CEDH de l'obtention des données concernées et de leur traitement ultérieur par les autorités britanniques[32].

---

26 CourEDH, arrêt *Big Brother Watch* précité, par. 381.

27 La CourEDH le relève elle-même, CourEDH, arrêt *Big Brother Watch* précité, par. 318.

28 Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, 2000/C 364/1 (ci-après la « Charte »).

29 CJUE, arrêt du 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12 (ci-après, « arrêt *Digital Rights Ireland* ») ; arrêt du 21 décembre 2016, *Tele2 Sverige AB*, C-203/15 et C-698/15 (ci après, « arrêt *Tele2 Sverige* ») ; cf. également section III ci-dessous.

30 Question préjudicielle du 31 octobre 2017, C-623/17.

31 CourEDH, arrêt *Big Brother Watch*, par. 420 s.

32 *Ibid*.

[Rz 19] S'appuyant largement sur la jurisprudence existante en matière d'interception massive[33], la CourEDH a retenu qu'en matière de réception de renseignements issus de la surveillance secrète par un Etat tiers, la base légale accessible au public devait prévoir au moins les éléments suivants[34] :

1. les conditions auxquelles les services de renseignements peuvent demander à un Etat tiers de leur communiquer des données interceptées ;
2. la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ;
3. les précautions à prendre pour la communication des données à d'autres parties ; et
4. les circonstances dans lesquelles la destruction des enregistrements s'impose.

[Rz 20] Il s'agit en substance des mêmes points que dans le domaine de l'interception massive[35], adaptés aux circonstances particulières de la réception de renseignements. Plus précisément, les éléments qui relèvent de l'Etat tiers procédant à la surveillance (soit la détermination des catégories de personnes susceptibles d'être surveillées et la durée maximale de la surveillance[36]) ne doivent pas nécessairement figurer dans la loi de l'Etat récepteur. En outre, en matière d'échange de renseignements, la loi doit prévoir non seulement les infractions susceptibles de donner lieu à la demande d'échange de renseignements, mais aussi, plus largement, les circonstances dans lesquelles une telle demande peut s'inscrire. Il convient en effet de limiter la discrétion des autorités en la matière, pour éviter que l'échange de renseignements permette de contourner les restrictions à la surveillance domestique[37].

[Rz 21] L'arrêt *Big Brother Watch* examine uniquement la conventionnalité de la réception de renseignements par les autorités d'un Etat partie à la CEDH. Il ne traite pas de la remise d'informations à des autorités tierces. 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'Etat partie effectuerait l'interception, il nous semble que la loi devrait prévoir la nature des infractions susceptibles de donner lieu à un mandat d'interception, les catégories de personnes susceptibles d'être surveillées, et la durée maximale de la surveillance lorsque l'interception intervient à la demande d'un Etat tiers[38].

[Rz 22] En outre, selon nous, l'Etat tiers devrait présenter certaines garanties quant à l'utilisation, la communication ultérieure et la destruction des renseignements communiqués[39]. Dans ce contexte, nous relevons que dans le cas d'espèce, l'arrêt *Big Brother Watch* prend en considération les garanties applicables au traitement des données reçues. Selon le même raisonnement, la possibilité de communiquer des renseignements devrait à notre sens prendre en compte les règles de protection des données applicables dans l'Etat de destination et pourrait s'intéresser à

33 CourEDH, arrêt *Big Brother Watch*, par. 307 et 42 s. ; arrêt *Liberty* précité par. 62 ; et arrêt *Weber* précité, par. 95 ; cf. également section I.b ci-dessus.

34 CourEDH, arrêt *Big Brother Watch*, par. 423 s.

35 *Idem*, cf. points 4–6 énumérés sous section I.b.

36 Cf. points 2 et 3 énumérés sous section I.b

37 CourEDH, arrêt *Big Brother Watch*, par. 424.

38 Soit les points 1–3 énumérés sous section I.b.

39 Soit les points 4–6 énumérés sous section I.b.

la conformité de ces dernières aux instruments pertinents du Conseil de l'Europe, notamment la Convention 108[40].

c. Proportionnalité

[Rz 23] L'analyse de la CourEDH quant à la proportionnalité de l'échange de renseignements[41] reflète pour l'essentiel les mêmes exigences qu'en matière d'interception massive. Nous renvoyons dès lors aux développements qui précèdent à ce sujet[42].

III. L'obtention de données secondaires auprès de fournisseurs de télécoms

a. Remarques liminaires

[Rz 24] Les données secondaires de communications permettent de déterminer quels utilisateurs sont entrés en contact, ainsi que le lieu et le moment des communications (qui, où et quand), à l'exclusion du contenu de ces communications.

[Rz 25] Dans l'arrêt *Big Brother Watch*, la CourEDH a analysé pour la première fois à quelles conditions les services de renseignements pouvaient accéder à de telles données sans violer le droit à la vie privée et familiale.

b. Légalité

[Rz 26] À titre liminaire, la CourEDH a relevé que sous l'angle du droit de l'Union européenne, la question de l'accès par les autorités nationales aux données secondaires de communications avait fait l'objet de plusieurs arrêts de la CJUE[43]. Dans ces arrêts, la CJUE a notamment retenu que l'accès des autorités à de telles données devait 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 était strictement nécessaire pour lutter contre de graves infractions[44].

[Rz 27] La CourEDH a ensuite rappelé que le Royaume-Uni étant membre de l'Union européenne, l'ordre juridique de l'Union, y compris la jurisprudence de la CJUE susvisée, faisait partie intégrante de son ordre juridique. En cas de conflit entre le droit national et celui de l'Union, ce dernier prévaut.

---

40 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel conclue le 28 janvier 1981, entrée en vigueur pour la Suisse le 1er février 1998 (RS 0.235.1). La CourEDH n'a pas juridiction pour vérifier le respect de la Convention 108, mais a parfois pris en compte les principes de cette convention pour analyser le respect de l'art. 8 CEDH ; cf. p. ex. CourEDH, arrêt *Z. c. Finlande* du 25 février 1997, 22009/23, par. 95.

41 CourEDH, arrêt *Big Brother Watch*, par. 445 s.

42 Section I.c. Au Royaume-Uni, des garanties procédurales similaires s'appliquent en effet à l'interception de communications sur sol national et à la requête de renseignements auprès d'une autorité étrangère.

43 CourEDH, arrêt *Big Brother Watch*, par. 463 et par. 465 ss. Cf. CJUE, décision *Digital Rights Ireland* et décision *Tele2 Sverige*.

44 CJUE, arrêt *Tele2 Sverige* précité, par. 114–125 et arrêt *Digital Rights Ireland* précité par. 60–62.

[Rz 28] 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[45]. En effet, cette loi ne soumettait pas l'accès aux données à un contrôle indépendant préalable[46]. Par ailleurs, dans le domaine du droit pénal, l'IPA ne limitait pas les possibilités d'accès à la lutte contre les infractions graves[47].

[Rz 29] Dans la mesure où l'IPA n'était pas conforme au droit communautaire supérieur, la CourEDH a retenu qu'il n'existait pas de base légale nationale valide pour l'obtention des données secondaires de communications par les services secrets britanniques[48]. L'ingérence n'était dès lors pas admissible au regard de l'art. 8 al. 2 CEDH.

[Rz 30] Il sied de souligner que dans les considérants résumés ci-dessus, la CourEDH a examiné uniquement la légalité de l'ingérence, soit la conformité de la base légale invoquée à une source supérieure de droit domestique (*largo sensu*). 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, l'arrêt *Big Brother Watch* retient d'ailleurs qu'un contrôle indépendant préalable n'est pas indispensable au regard de l'art. 8 al. 2 CEDH[49].

[Rz 31] 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[50] conféraient une protection plus étendue que l'art. 8 CEDH[51]. Cela étant, l'analyse de la CJUE s'opérait exclusivement au regard de la Charte[52]. La CJUE a considéré par le passé que la jurisprudence de la CourEDH ne pouvait imposer aux organes de l'Union européenne une interprétation déterminée des règles du droit communautaire, y compris de la Charte[53]. Le législateur européen s'est au demeurant prononcé en faveur d'un cadre de protection des données solide au sein de l'Union européenne en adoptant un nouvel instrument communautaire en la matière, le RGPD[54]. Dans ces circonstances, nous nous attendons à ce que la CJUE maintienne sa jurisprudence nonobstant l'arrêt de la CourEDH commenté ici. Si tel est le cas, 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. L'arrêt *Big Brother Watch* signifie ainsi vraisemblablement la fin d'une période de convergence[55] de la jurisprudence des deux Cours.

45 *High Court of Justice*, décision 2018 EWHC 975 (Admin) du 27 avril 2018.

46 *Ibid*.

47 *Ibid*.

48 CourEDH, arrêt *Big Brother Watch*, par. 466 et 467.

49 CourEDH, arrêt *Big Brother Watch*, par. 466 ss, cf. section I.c.

50 Art. 7 et 8 de la Charte.

51 CJUE, arrêt *Tele2 Sverige* précité, par. 126–133 ; plus succinctement arrêt *Digital Rights Ireland* précité, par. 72.

52 *Ibid*.

53 CJUE, avis 2/13 du 18 décembre 2014 relatif au projet d'adhésion de l'Union européenne à la CEDH.

54 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

55 Par le passé, la CourEDH s'est appuyée sur la jurisprudence de la CJUE et réciproquement, cf. p. ex. CourEDH, arrêt *Szabo* précité, par. 23, 24 et 73 ; CJUE, arrêt *Digital Rights Ireland* précité, par. 54.

c. Digression : la conservation indiscriminée des données secondaires par les fournisseurs de télécoms

[Rz 32] La conservation des données secondaires de communications par les opérateurs, qui constituait la question centrale des arrêts *Digital Rights Ireland* et *Tele2 Sverige* précités de la CJUE, n'était pas litigieuse devant la CourEDH en l'espèce. A 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 à notre avis tirer certains enseignements de la jurisprudence existante de la CourEDH, y compris la position adoptée ici en matière d'interception massive[56].

[Rz 33] En effet, la CourEDH a retenu qu'en tant que telle, l'interception de larges catégories de communications n'excluait pas la conformité de la surveillance à l'art. 8 CEDH[57]. En outre, à teneur de jurisprudence, l'interception de données secondaires représente par nature une atteinte moindre au droit à la vie privée que l'interception du contenu des communications[58]. Dans ce contexte, la CourEDH a jusqu'ici considéré que seule l'exploitation des données conservées par les opérateurs (et non la conservation en tant que telle) représentait une ingérence dans l'exercice du droit à la vie privée[59]. Selon nous, au regard de cette jurisprudence, la conservation indiscriminée de vastes volumes de données secondaires de communication peut être compatible avec la CEDH, pour autant qu'elle soit prévue par la loi, vise la sauvegarde d'intérêts légitime et soit proportionnée (cf. art. 8 al 2. CEDH). Sous l'angle de la proportionnalité, la conservation devra en particulier être limitée dans le temps et ne pas résulter en un risque de stigmatisation[60]. L'accès des autorités aux données devra également répondre aux exigences de l'art. 8 al. 2 CEDH[61].

[Rz 34] Par opposition, la CJUE a jugé qu'en tant que telle, la conservation indiscriminée de l'ensemble des données de communications pendant plusieurs mois constituait une ingérence disproportionnée dans l'exercice des droits garantis par la Charte, notamment au motif que cette

56 Cf. section I.

57 CourEDH, arrêt *Big Brother Watch*, par. 338.

58 CourEDH, arrêt *Big Brother Watch* précité, par. 462 ; arrêt *P.G. et J.H. c. Royaume-Uni* du 25 septembre 2001 44787/98, par. 42 ; et arrêt *Malone et al. c. Royaume Uni* du 2 août 1984, 8691/79, par. 84. De façon similaire, la CourEDH a considéré que la surveillance par géolocalisation est en général moins susceptible de porter atteinte à la vie privée de la personne concernée que la surveillance par des moyens visuels ou acoustiques, ces dernières révélant davantage d'informations sur la conduite, les opinions ou les sentiments de cette personne (CourEDH, arrêt *Ben Faiza c. France* du 8 février 2018, 31446/12, par. 53 ; et arrêt *Uzun c. Allemagne* du 2 septembre 2010, 35623/05, par. 52). Par opposition, la CJUE a estimé que la conservation de l'ensemble des données de communications pendant plusieurs mois constituait une ingérence particulièrement grave dans l'exercice du droit à la vie privée (CJUE, arrêt *Digital Rights Ireland* précité, par. 39).

59 CourEDH, arrêt *Figueiredo Teixeira c. Andorre* du 8 novembre 2016, 72384/14, par. 40 ; et arrêt *Malone* précité, par. 83 s. Précisons que dans un contexte différent, soit la conservation d'échantillons cellulaires et profils ADN et d'empreintes digitales de personne qui avaient été soupçonnées d'infractions pénales, la CourEDH a admis que la conservation de données personnelles en tant que telle pouvait constituer une ingérence au sens de l'art. 8 al. 2 CEDH (CourEDH, arrêt *S. et Marper c. Royaume-Uni* du 4 décembre 2008, 30562/04 et 30566/04, par. 67 s.). Cela étant, sous l'angle de la proportionnalité de cette inférence, la Cour a principalement pris en compte le risque de stigmatisation lié à l'inscription dans la base de données litigieuse et l'absence de limite à la durée de conservation (CourEDH, arrêt *S. et Marper* précité, par. 118 ss). En l'espèce, le risque de stigmatisation découlait du fait que seules les données d'individus condamnés ou acquittés étaient conservées dans la base de données, alors que les données concernant des personnes n'ayant jamais été soupçonnées d'une infraction étaient détruites.

60 Cf. CourEDH, arrêt *S. et Marper* précité, par. 118 s.

61 Cf. notamment section III.b.

mesure ne présupposait aucun lien entre les données conservées et les menaces envers la sécurité publique contre lesquelles elle était censée lutter[62].

[Rz 35] 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[63] était conforme au droit à la vie privée garanti par l'art. 8 CEDH[64]. Il a expressément exclu la possibilité de transposer directement la jurisprudence de la CJUE susvisée au droit suisse et a retenu que le régime suisse était conforme à la CEDH, au regard des conditions strictes posées par le CPP[65] pour l'accès aux données. A 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.

Conclusion

[Rz 36] L'arrêt *Big Brother Watch* marque une étape jurisprudentielle importante. A notre connaissance, il s'agit de l'analyse la plus complète d'un système de surveillance étatique généralisée effectuée à ce jour par la CourEDH. Dans cet arrêt, la CourEDH se prononce d'ailleurs pour la première fois sur certains aspects d'un tel système de surveillance, en particulier l'échange d'informations avec des pays tiers et l'obtention de données secondaires de communication. Si les exigences formulées à cet égard reposent largement sur la jurisprudence existante, l'arrêt *Big Brother Watch* marque un tournant à certains points de vue.

[Rz 37] En particulier, la CourEDH renonce dans cet arrêt à exiger systématiquement un contrôle indépendant préalable de l'interception massive de communications. Ainsi, loin de marquer une victoire des défenseurs de la vie privée (comme prétendu par certains sur les réseaux sociaux), l'arrêt *Big Brother Watch* marque l'érosion d'une importante exigence formelle, articulée de longue date par la jurisprudence. Comme précédemment mentionné, cette évolution nous semble regrettable. En outre, il en résulte une lisibilité moindre des critères appliqués par les juges de Strasbourg quant à l'existence de garanties suffisantes. Selon nous, une si vaste marge d'appréciation est peu opportune dans un domaine politiquement sensible comme celui de la surveillance étatique.

[Rz 38] Par ailleurs, ce développement va à l'encontre de l'évolution de la jurisprudence communautaire sous l'angle de la Charte européenne, la CJUE s'étant montrée très stricte dans ses récentes décisions en matière de surveillance généralisée. Comme précédemment évoqué, ceci laisse présager une évolution divergente de la jurisprudence de la CourEDH et de la CJUE, notamment concernant l'admissibilité de la conservation massive des données secondaires (sur laquelle la CourEDH ne s'est à notre connaissance pas encore prononcée) et celle de l'interception de masse (concernant laquelle une question préjudicielle est actuellement pendante devant la CJUE).

[Rz 39] L'arrêt *Big Brother Watch* n'est pas définitif, la CourEDH ayant admis une demande de renvoi de l'affaire devant la Grande Chambre. La portée de cette jurisprudence reste ainsi à confir-

62 CJUE, arrêts*Tele2 Sverige*, par. 106 s. et arrêt *Digital Rights Ireland* précité, par. 58 s.

63 Art. 15 al. 3 aLSCPT, actuellement art. 26 al. 5 LSCPT.

64 ATF 144 I 126 ; résumé in : Emilie Jacot-Guillarmod, L'enregistrement systématique des données secondaires de communication, in : www.lawinside.ch/600/.

65 Art. 197 ss et 269 ss CPP.

mer. Nous formulons ici l'espoir que la Grande Chambre pose des exigences plus strictes en la matière. Quelle que soit l'issue de la cause, au vu de l'ampleur des questions traitées *in casu*, l'affaire *Big Brother Watch* est susceptible de marquer durablement la jurisprudence relative à la surveillance de masse par les Etats parties à la CEDH.

Emilie Jacot-Guillarmod est avocate et éditrice auprès de LawInside.ch. Elle pratique au sein du barreau genevois et conseille notamment des clients en matière de protection des données et de contrats informatiques.

L'auteure remercie infiniment Me Aurélie Cachelin pour sa prompte relecture et ses commentaires avisés.