La Cour européenne des droits de l'homme et la surveillance de masse

PAR

François DUBUISSSON

Professeur à l'Université libre de Bruxelles
Centre de droit international

Résumé

La présente contribution analyse l'évolution de la jurisprudence de la Cour européenne des droits de l'homme relative à l'évaluation de la compatibilité des régimes juridiques de surveillance mis en place par les États, au regard du respect du droit à la vie privée et de la liberté d'expression et d'information. Il est montré que les spécificités de la surveillance de masse appellent un contrôle plus strict, comme la Cour l'a énoncé pour la première fois dans son arrêt *Szabó et Vissy c. Hongrie*.

Abstract

This contribution analyzes the evolution of the case-law of the European Court of Human Rights on the examination of the compatibility of surveillance regimes set up by States under the right to privacy and freedom of expression and information. It is shown that the specific characteristics of mass surveillance call for stricter control, as the Court stated for the first time in its judgment *Szabó and Vissy c. Hungary*.

La question de la compatibilité avec les droits fondamentaux d'activités de surveillance mises en œuvre par les services de sécurité des États est soulevée depuis longtemps déjà, et a fait l'objet d'une abondante jurisprudence de la part de la Cour européenne des droits de l'homme. Avec l'évolution des technologies, le champ et la portée des mesures de surveillance se sont considérablement accrus, conjointement avec le développement de législations visant à accroître les moyens à disposition des services de renseignement en vue de lutter contre

le terrorisme, après les attentats du 11 septembre 2001. La surveillance a ainsi pris un caractère potentiellement massif, alliant des mesures ciblées visant des individus identifiés à des récoltes générales et prospectives de données, notamment dans le cadre des réseaux numériques[1]. Cette évolution a été particulièrement mise en évidence à la suite des révélations faites par Edward Snowden concernant la mise en œuvre des programmes de la National Security Agency (NSA), impliquant l'interception des télécommunications internationales (programme « Échelon ») et le traitement de données détenues par les opérateurs et les fournisseurs de services sur internet (programme « Prism »)[2].

Ces informations ne sont pas restées sans conséquences. L'Assemblée générale des Nations Unies a adopté en décembre 2013 une résolution sur le « droit à la vie privée à l'ère du numérique »[3], qui déclare que « la surveillance illicite ou arbitraire ou l'interception des communications, ainsi que la collecte illicite ou arbitraire de données personnelles, qui sont des actes extrêmement envahissants, portent atteinte aux droits à la vie privée et à la liberté d'expression et pourraient aller à l'encontre des principes de toute société démocratique ». Diverses instances internationales compétentes dans le domaine des droits de l'homme ont adopté des rapports analysant la compatibilité des mesures de surveillance massive avec les des droits de l'homme, et la Cour de justice de l'Union européenne a rendu deux arrêts abordant également cette problématique[4].

---

[1] Le concept de « surveillance de masse » est aujourd'hui couramment utilisé dans les rapports internationaux (voy. les rapports analysés *infra*), même s'il ne fait pas l'objet d'une définition formelle. Il vise la récolte stratégique et prospective de données concernant des personnes qui ne sont pas directement soupçonnées d'être liées à la commission d'actes criminels ou d'activités mettant en cause la sécurité nationale, ou de personnes faisant partie d'un cercle restreint autour d'une personne suspecte. Nous utiliserons également de manière équivalente les termes de surveillance « générale » et « non ciblée », même si divers degrés peuvent exister dans l'étendue des mesures de renseignement.

[2] Voy. F. Dubuisson, « Chronique : société de l'information, médias et liberté d'expression », *Journal européen des droits de l'homme*, 2014/3, pp. 359 et s.

[3] Assemblée générale des Nations Unies, « Le droit à la vie privée à l'ère du numérique », A/RES/68/167, 18 décembre 2013. Voy. aussi Assemblée générale des Nations Unies, « Le droit à la vie privée à l'ère du numérique », A/RES/69/166, 18 décembre 2014 ; Conseil des droits de l'homme des Nations Unies, « Le droit à la vie privée à l'ère du numérique », Résolution 28/16, 1er avril 2015.

[4] C.J.U.E., Gde ch., arrêt *Digital Rights Ireland Ltd (C-293/12) c. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung (C-594/12) e.a.*, 8 avril 2014 ; C.J.U.E., Gde Ch., arrêt *Maximillian Schrems c. Data Protection Commissioner*, 6 octobre 2015, C-362/14.

Il était donc intéressant de voir si, à la lumière de ces développements, la Cour européenne des droits de l'homme allait faire évoluer sa jurisprudence pour l'adapter aux caractéristiques particulières de la surveillance non ciblée, de nature plus intrusive. L'occasion lui en était donnée à travers l'examen de deux requêtes, visant les lois russe et hongroise octroyant de larges pouvoirs aux services de renseignement concernant la récolte de données relatives à des personnes n'étant pas suspectées d'actes criminels (affaires *Roman Zakharov c. Russie* et *Szabó et Vissy c. Hongrie*). Pour analyser avec précision la portée des décisions rendues dans ces deux affaires, il est nécessaire d'exposer préalablement la jurisprudence classique de la Cour dans le domaine de la surveillance (I), puis d'examiner l'apport des travaux récents des organes des Nations Unies et de la jurisprudence de la Cour de justice de l'Union sur cette question, ayant examiné l'impact de la surveillance de masse sur les droits fondamentaux (II). Nous montrerons ainsi que les deux récents arrêts de la Cour européenne des droits de l'homme ont adopté des approches différentes de la définition des critères de compatibilité de la surveillance non ciblée avec les droits fondamentaux (III). Alors que la Grande Chambre est restée fidèle à la jurisprudence traditionnelle, en reconnaissant à l'État « une ample marge d'appréciation » dans le choix des moyens de sauvegarder la sécurité nationale (*Roman Zakharov c. Russie*), la Cour a opté dans l'affaire *Szabó et Vissy c. Hongrie*, pour une approche plus spécifique de la surveillance de masse, retenant un critère de conventionnalité plus exigeant, inspiré des rapports des Nations Unies et des arrêts de la Cour de justice de l'Union européenne.

I. La jurisprudence traditionnelle de la Cour européenne des droits de l'homme : la reconnaissance d'une « ample marge d'appréciation »

La Cour européenne des droits de l'homme a développé une assez abondante jurisprudence concernant la compatibilité avec la Convention des mesures de surveillance, fondée principalement sur le précédent *Klass e.a. c. Allemagne* établi en 1978[5]. Dans cette affaire, cinq ressortissants allemands prétendaient que leur droit à la vie privée était violé du fait de l'existence d'une législation dite « G10 », autorisant certaines autorités à adopter des mesures de surveillance sans que la personne visée n'en soit jamais avertie ni n'ait la possibilité de saisir les tribunaux, une fois les mesures levées. Après avoir reconnu aux requérants la qualité de « victimes » en constatant que « la législation incriminée institue un système de surveillance exposant chacun, en République fédérale

[5] Cour eur. dr. h., arrêt *Klass e.a. c. Allemagne*, 6 septembre 1978.

d'Allemagne, au contrôle de sa correspondance, de ses envois postaux et de ses télécommunications, sans qu'il le sache jamais à moins d'une indiscrétion ou d'une notification ultérieure »[6], la Cour a établi les principes à suivre dans l'évaluation de la compatibilité d'un régime juridique de surveillance avec l'article 8 de la Convention. Il faut tout d'abord que l'ingérence ait été prévue par la loi, ce qui suppose qu'elle résulte « de lois adoptées par le parlement » et que « toute mesure individuelle de surveillance doive se conformer aux conditions et procédures rigoureuses fixées par la législation elle-même »[7]. Il faut ensuite que le système de surveillance soit, dans une société démocratique, « nécessaire à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales », ce qui suppose de vérifier « si les moyens prévus par la législation en cause pour atteindre ce but restent à tous égards à l'intérieur des bornes de ce qui est nécessaire dans une société démocratique »[8]. À cet égard, la Cour a reconnu une légitimité de principe à l'utilisation de mesures de surveillance à des fins de sécurité nationale : « Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. La Cour doit donc admettre que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales. »[9]

Elle en a dès lors déduit que s'agissant de définir les modalités du système de surveillance, « le législateur national jouit d'un certain pouvoir discrétionnaire »[10]. Cette marge d'appréciation n'est toutefois pas « illimitée »[11], ce qui implique que la Cour examine « l'existence de garanties adéquates et suffisantes contre les abus »[12]. Cette appréciation doit se faire compte tenu « de toutes les circonstances de la cause », en particulier « l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne »[13].

[6] *Ibid.*, § 37.
[7] *Ibid.*, § 43.
[8] *Ibid.*, § 46.
[9] *Ibid.*, § 48.
[10] *Ibid.*, § 49.
[11] *Ibid.*
[12] *Ibid.*, § 50.
[13] *Ibid.*

Ce sont ces principes et ces critères qui seront repris par la Cour par la suite pour évaluer la compatibilité avec les droits consacrés par la Convention, en particulier le droit à la vie privée (article 8) et le droit à la liberté d'expression et d'information (article 10), des régimes de surveillance mis en place par les États. Cette évaluation s'est traduite par une analyse tant de l'exigence de légalité (A) que des conditions de nécessité et proportionnalité (B).

A. *L'exigence de légalité appliquée aux régimes de surveillance*

Les implications de l'exigence de légalité dans le contexte des mesures de surveillance n'avaient guère été explicitées dans l'affaire *Klass*, mais ont été définies dans certaines affaires ultérieures. Selon la jurisprudence de la Cour, la condition de légalité suppose non seulement que les mesures de surveillance disposent d'un fondement légal, mais également que la loi soit suffisamment accessible et prévisible pour les citoyens[14]. Dans la mesure où les mesures de surveillance sont généralement décidées par les services de renseignement de manière secrète, à l'insu des personnes surveillées, les conditions d'accessibilité et de prévisibilité ont pris une dimension particulière. C'est ce qu'a souligné la Cour européenne des droits de l'homme dans l'affaire *Weber et Saravia c. Allemagne* :

> « Quant à [l'] exigence [de] […] prévisibilité de la loi, la Cour rappelle que dans le contexte particulier des mesures de surveillance secrète, telles que l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même d'escompter quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence. [Cependant], le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes.
>
> […] En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire. »[15]

[14] Cour eur. dr. h., arrêt *Kennedy c. Royaume-Uni*, 18 mai 2010, § 155.

[15] Cour eur. dr. h., décision *Weber et Saravia c. Allemagne*, 29 juin 2006, §§ 93-94.

La loi organisant le régime du renseignement doit donc comporter un certain nombre de précisions et de définitions minimales énumérées par la Cour de la manière suivante :

> « […] la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements. »[16]

Ces critères ont amené la Cour à juger que la loi allemande du 28 octobre 1994 sur la lutte contre la criminalité, qui était mise en cause dans l'affaire *Weber et Saravia*, satisfaisait à l'exigence de légalité. Elle contenait, selon la Cour, une définition claire et précise des infractions pour la prévention desquelles l'interception stratégique de télécommunications pouvait être ordonnée[17]. Elle indiquait les catégories de personnes susceptibles de faire l'objet d'écoutes téléphoniques (les personnes concernées devaient notamment avoir participé à une conversation téléphonique internationale par l'intermédiaire de relais satellites ou hertziens, en employant des mots clés de nature à déclencher une enquête sur certains dangers énumérés par la loi)[18]. Une durée maximale des écoutes était fixée (délai de trois mois, renouvelable si les mêmes conditions prévalent)[19]. La procédure à suivre pour l'examen et l'utilisation des données recueillies étaient régies avec précision[20]. Enfin, la loi exposait en détail les modalités de destruction de données obtenues au moyen d'une surveillance stratégique[21].

À l'inverse, la condition de légalité a été considérée par la Cour européenne des droits de l'homme comme n'étant pas satisfaite par la loi britannique dans l'affaire *Liberty e.a. c. Royaume-Uni*, qui a donné lieu à un arrêt du 1er juillet 2008[22]. En l'espèce, la loi de 1985 sur l'interception de communications (*Interception of Communications Act 1985*), révisée en 2000, permettait d'intercepter « les communications à destination ou provenance de l'étranger mentionnées

[16] *Ibid.*, § 95.
[17] *Ibid.*, § 97
[18] *Ibid.*
[19] *Ibid.*, § 98.
[20] *Ibid.*, § 99.
[21] *Ibid.*, § 100.
[22] Cour eur. dr. h., arrêt *Liberty e.a. c. Royaume-Uni*, 1er juillet 2008.

dans [un] mandat »[23] et ne prévoyait aucune restriction quant aux catégories de communications pouvant y figurer. Il était prévu que les données interceptées pouvaient être écoutées ou lues, « dès lors que le ministre de l'Intérieur jugeait leur examen nécessaire à protection de la sécurité nationale, à la prévention d'infraction graves ou à la sauvegarde des intérêts de l'économie britannique »[24]. Le recours avait été introduit par trois associations de défense des libertés civiles, dont les communications entre Dublin et Londres avaient été interceptées.

Au regard du flou des dispositions législatives et de la très grande marge de manœuvre laissée au ministre de l'Intérieur, la Cour a estimé que le régime normatif britannique ne répondait pas à l'exigence de légalité :

> « En définitive, la Cour considère que, faute d'avoir défini avec la clarté requise l'étendue et les modalités d'exercice du pouvoir d'appréciation considérable conféré à l'État en matière d'interception et d'analyse des communications à destination ou en provenance de l'étranger, la loi en vigueur à l'époque pertinente n'offrait pas une protection suffisante contre les abus de pouvoir. En particulier, au rebours de ce qu'exige la jurisprudence de la Cour, aucune précision sur la procédure applicable à l'examen, la diffusion, la conservation et la destruction des données interceptées n'y figurait sous une forme accessible au public »[25].

Dans le même temps, la Cour a rejeté l'argument du Royaume-Uni tiré des nécessités du secret lié aux opérations de renseignement, en se référant au précédent *Weber et Saravia* :

> « Le gouvernement avance que la divulgation d'informations sur les mesures relatives à l'examen, l'utilisation, la conservation et la destruction de renseignements interceptés prises par le ministre de l'Intérieur à l'époque pertinente aurait pu nuire à l'efficacité du dispositif de collecte de données ou créer un risque pour la sécurité. Toutefois, [la Cour] observe que les autorités allemandes ont considéré que l'insertion, dans la loi G10 en cause dans l'affaire *Weber et Saravia* (précitée), de dispositions expresses sur le traitement de données obtenues au moyen d'interceptions stratégiques pratiquées sur des lignes téléphoniques non allemandes ne présentait pas de danger. »[26]

[23] *Ibid.*, § 64.
[24] *Ibid.*, § 24.
[25] *Ibid.*, § 69.
[26] *Ibid.*, § 68.

Il résulte donc de la jurisprudence de la Cour que les mesures de surveillance doivent être encadrées par un système légal qui en définisse de manière suffisamment précise les contours.

Le test de légalité s'avère donc, pour les programmes de renseignement, dépasser l'exigence purement formelle pour nécessiter la définition suffisamment précise d'une série de conditions substantielles concernant les modalités de décision et de mise en œuvre de mesures de surveillance, qu'elles soient ciblées ou massives.

Dans la suite de sa jurisprudence, la Cour a opté pour un certain changement de méthode d'analyse en abandonnant tout examen spécifique de l'exigence de légalité, lorsqu'est mis en cause un régime légal de surveillance dans son ensemble, et non l'adoption de telle mesure particulière à l'encontre d'un individu :

> « la question de la légalité de l'ingérence est étroitement liée à celle de savoir si le régime institué par la [loi] satisfait au critère de la 'nécessité', raison pour laquelle la Cour doit examiner conjointement les critères de la 'prévisibilité au regard de la loi' et de la 'nécessité' »[27].

Dans cette optique, la question de la « légalité » se fond dans la condition de « nécessité », et appelle à une analyse conjointe des deux conditions, qui consiste à évaluer la proportionnalité du régime de surveillance, au regard des buts légitimes poursuivis.

B. *L'exigence de proportionnalité appliquée aux régimes de surveillance*

Au regard de la Convention européenne des droits de l'homme, les limitations apportées à l'exercice des droits à la vie privée et à la liberté d'expression doivent apparaître comme étant proportionnées au regard des objectifs publics poursuivis. Cela signifie que les activités de surveillance ne peuvent s'ingérer dans la vie privée et la liberté d'expression des individus que dans la mesure nécessaire à la protection de certains intérêts reconnus comme légitimes. Le contrôle qui est réalisé à cet effet s'appuie sur différents critères mis en évidence par la jurisprudence de la Cour[28]. En particulier, les principaux variables à

[27] Cour eur. dr. h., arrêt *Kennedy c. Royaume-Uni*, précité, § 155.

[28] Voy. aussi M. Milanovic, « Human Rights Treaties and Foreign Surveillance : Privacy in the Digital Age », *Harvard International Law Journal,* 2015, vol. 56, pp. 133 et s.

prendre en considération sont les suivants : la nature du but poursuivi, la portée de la mesure de surveillance, les conditions d'utilisation des données récoltées, les mécanismes de contrôle et de recours existants. Comme on le verra, la jurisprudence classique de la Cour n'a pas, dans la mise en œuvre de ces critères, pris en considération les spécificités des mesures de surveillance non ciblées.

1. Le but poursuivi par la mesure de surveillance

La Convention européenne des droits de l'homme permet l'adoption de mesures de restriction de la vie privée et de la liberté d'expression nécessaires à la poursuite de divers buts légitimes, dont la sécurité nationale, l'ordre public, la prévention des infractions, l'intégrité territoriale, le bien-être économique du pays, la protection des droits d'autrui. Ces buts offrent un spectre assez large qui donne de prime abord un large pouvoir d'appréciation dans le chef de l'État dans la détermination des objectifs permettant de mener des activités de renseignement. Toutefois, la nature du but invoqué pour fonder des actes de surveillance devrait être de nature à influencer l'analyse de la proportionnalité des mesures de surveillance prises dans la poursuite de ce but. On peut penser que la lutte contre le terrorisme autorisera des ingérences plus intrusives que la protection du bien-être économique, par exemple.

Cette question n'a, jusqu'à présent, pas été abordée de manière directe dans la jurisprudence de la Cour. Dans l'affaire *Weber et Saravia,* la loi allemande G10 ne visait que des hypothèses étroitement liées à la prévention du crime et à la protection de la sécurité nationale (attaque armée contre la République fédérale d'Allemagne, terrorisme, trafic international d'armes, trafic de stupéfiants, faux-monnayage, blanchiment d'argent)[29] et les requérants ne mettaient pas en cause l'existence d'un but légitime, ce qui a conduit la Cour a accepter le point de vue de l'Allemagne sans discussion particulière[30]. Dans l'affaire *Liberty e.a.*, la loi britannique mentionnait comme motifs permettant la mise en place d'opération de surveillance, outre « la sécurité nationale » et « la prévention et la détection d'infractions graves », « la sauvegarde du bien-être économique du Royaume-Uni » qui constitue un objectif conçu de manière extrêmement large et ne renvoyant pas nécessairement ni à des impératifs de sécurité ni à la commission d'infractions pénales. On pouvait dès lors se demander si un tel objectif entrait bien dans les prévisions des buts légitimes énoncés par la Convention (le « bien-être économique du pays » est bien repris comme motif de limitation à l'article 8, mais pas à l'article 10 pour la liberté d'expression)

[29] Voy. Cour eur. dr. h., décision *Weber et Saravia c. Allemagne*, précité, § 27.
[30] *Ibid.*, §§ 103-104.

et surtout s'interroger sur le type de mesures qu'une telle finalité autorise, de manière autonome, sous l'angle de la proportionnalité[31]. La Cour n'a toutefois pas jugé utile d'examiner ce point de manière spécifique.

2. La portée de la mesure de surveillance

Un second paramètre à prendre en considération dans l'appréciation de la proportionnalité de la mesure de surveillance est la portée de celle-ci. Les moyens de surveillance ont évolué de manière extraordinaire ces vingt dernières années, principalement en corrélation avec le développement des technologies numériques et d'internet. On est ainsi passé de mesures ciblées, consistant principalement en l'interception de conversations téléphoniques fixes et du courrier, en l'utilisation de balises ou encore en l'observation directe, à la mise en œuvre de techniques beaucoup plus perfectionnées permettant de tracer les nombreux agissements d'un individu par l'entremise de son téléphone portable ou de ses navigations sur Internet. À cette surveillance ciblée de plus en plus sophistiquée, se sont ajoutées des facultés de récoltes et de traitements massifs de données à des fins stratégiques, en vue d'identifier parmi celles-ci des éléments permettant d'identifier des comportements suspects ou de retrouver des informations concernant des infractions commises. L'évolution technologique entraîne donc des ingérences dans la vie privée et la liberté d'expression qui sont potentiellement de plus en plus intrusives et qui sont susceptibles de concerner des personnes qui n'ont commis et qui ne commettront aucun délit[32].

Pourtant, la Cour a choisi de ne pas intégrer dans son raisonnement la question de la portée de la mesure de surveillance. Dans l'affaire *Liberty e.a. c. Royaume-Uni*, elle a indiqué qu'elle « ne voit aucune raison de soumettre les règles gouvernant l'interception de communications individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents »[33]. L'affirmation de la Cour laisse entendre qu'il ne convient *a priori* pas de soumettre les mesures de surveillance à des critères de licéité différents selon qu'elles soient ciblées ou massives. On trouve une attitude identique dans

[31] Voy. M. Milanovic, *op. cit.*, p. 136.

[32] Voy. I. Brown et D. Korff, « Foreign surveillance : Law and Practice in a Global Digital Environment », *European Human Rights Law Review*, 2014, n° 3, pp. 243 et s. ; I. Georgieva, « The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR », *Utrecht Journal of International and European Law*, 2015, pp. 122-124 ; D. Yernault, « De la fiction à la réalité : le programme d'espionnage électronique global Échelon et la responsabilité internationale des États au regard de la Convention européenne des droits de l'homme », *Revue belge de droit international*, 2000, pp. 137 et s.

[33] Cour eur. dr. h., arrêt *Liberty e.a. c. Royaume-Uni*, précité, § 28.

l'affaire *Weber et Saravia c. Allemagne*, qui concernait des communications susceptibles d'être interceptées sur la base de mots clés, dans le cadre de ce qui constituait une activité de surveillance générale, ne ciblant pas des individus préalablement repérés comme présentant un risque pour la sécurité nationale. Les requérants mettaient en évidence le fait que « la surveillance automatique […] était d'une trop grande portée puisqu'elle n'aurait plus été soumise à aucune restriction géographique et qu'il aurait été possible d'identifier des personnes et, si celles-ci utilisaient des téléphones portables, de suivre leurs déplacements »[34]. De plus, elle pouvait viser des personnes « sans aucune raison ni aucun soupçon préalable »[35]. Ces éléments particuliers ont tout simplement été ignorés par la Cour dans son raisonnement concernant l'analyse de la proportionnalité. La Cour n'a examiné que les objectifs poursuivis par la loi (lutte contre une série d'infractions graves) et les modalités procédurales encadrant la prise de mesures[36], mais n'a pas évalué la nécessité et l'efficacité de l'utilisation d'un programme de détection de mots clés, s'appliquant à l'ensemble des télécommunications internationales avec l'Allemagne, susceptibles de toucher des personnes qui ne sont suspectées d'aucune infraction. Ce faisant, la Cour ne faisait que rappeler sa jurisprudence établie en 1978 dans l'affaire *Klass c. Allemagne*, dans laquelle elle avait reconnu au législateur allemand « un certain pouvoir discrétionnaire » quant aux « choix des modalités du système de surveillance »[37]. Comme nous le verrons, cette position s'est trouvée largement remise en cause par la jurisprudence de la Cour de justice de l'Union européenne et les rapports des instances de l'ONU, et elle donnera lieu à des vues divergentes dans les deux décisions relatives aux affaires *Roman Zakharov c. Russie* et *Szabó et Vissy c. Hongrie*.

3. Les conditions d'utilisation des données récoltées

Le troisième paramètre à prendre en compte pour l'évaluation de la proportionnalité des mesures de surveillance concerne la définition des conditions d'utilisation des informations récoltées. L'exigence de légalité suppose que ces conditions soient définies dans la loi avec une clarté et une prévisibilité suffisantes (voy. ci-dessus). Mais il faut encore que les conditions particulières d'interception, de conservation et d'utilisation des données apparaissent proportionnées au regard de l'objectif poursuivi.

---

[34] Cour eur. dr. h., décision *Weber et Saravia c. Allemagne*, précité, § 111.

[35] *Ibid.*

[36] *Ibid.*, §§ 114-117.

[37] Cour eur. dr. h., arrêt *Klass e.a. c. Allemagne*, précité, § 49.

Se plaçant dans le sillage de l'arrêt *Klass c. Allemagne*[38], la Cour a affirmé dans l'affaire *Weber et Saravia c. Allemagne* que le contrôle de proportionnalité devait se faire en reconnaissant une large marge d'appréciation à l'État, tout en vérifiant la présence de garanties suffisantes contre l'arbitraire :

> « La Cour rappelle que, lorsqu'elle doit mettre en balance l'intérêt de l'État défendeur à protéger la sécurité nationale au moyen de mesures de surveillance secrète et la gravité de l'ingérence dans l'exercice par un requérant de son droit au respect de sa vie privée, elle dit invariablement que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale. Néanmoins, elle doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre. Cette appréciation dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne »[39].

Cela s'est traduit en l'occurrence par un contrôle effectivement très marginal des conditions entourant le recours aux mesures de surveillance, telles que prévues par la loi allemande. La Cour a dès lors admis assez aisément le caractère proportionné et nécessaire du régime légal allemand, en observant qu'il contenait « une série de conditions restrictives [qui] doivent être remplies pour qu'une mesure entraînant une surveillance stratégique puisse être imposée »[40]. En particulier, la Cour a retenu le fait que la surveillance ne peut intervenir que dans le cas de certains faits criminels graves, pour une durée limitée (trois mois) et que les conditions d'utilisation, de transmission, de conservation et de destruction des données sont définies avec précision dans la loi[41]. Mais comme on l'a relevé plus haut, jamais la Cour n'a pris en compte la méthode utilisée et les catégories de personnes visées (en l'espèce, les requérants n'étaient pas soupçonnés d'être liés d'aucune façon à des activités criminelles) pour évaluer la proportionnalité du régime de surveillance.

[38] Cour eur. dr. h., arrêt *Klass e.a. c. Allemagne*, précité, § 49.
[39] Cour eur. dr. h., décision *Weber et Saravia c. Allemagne*, précité, § 106 (références omises).
[40] *Ibid.*, § 115.
[41] *Ibid.*, §§ 115 et s.

4. L'existence de mécanismes de contrôle et de recours suffisants

Le dernier élément pertinent pour évaluer la proportionnalité du régime de surveillance est l'existence de garanties procédurales par la mise en place de mécanismes de contrôle effectif. À cet égard, la surveillance pose une difficulté particulière puisqu'elle sera normalement décidée et mise en œuvre à l'insu de la personne intéressée, et ses modalités précises seront susceptibles de relever d'impératifs de sécurité nationale impliquant de les maintenir secrètes. Il est donc nécessaire de trouver un équilibre délicat entre les exigences d'efficacité des activités des services de renseignement et la garantie des droits des individus.

Dans l'affaire *Weber et Saravia c. Allemagne*, la Cour européenne des droits de l'homme a estimé suffisante l'existence d'un mécanisme de contrôle ou de réexamen ultérieur par deux organes non judiciaires : un comité parlementaire et une commission dite « G10 », composée d'un président ayant les qualités pour accéder à la magistrature et de deux assesseurs :

> « Quant à la supervision et au contrôle des mesures de surveillance, la Cour relève que la loi G10 les confie à deux organes indépendants ayant un rôle relativement important. Il s'agit, premièrement, du comité parlementaire de contrôle, composé de neuf membres du Parlement, y compris des représentants de l'opposition. Le ministre fédéral qui autorise des mesures de surveillance doit rendre compte à ce comité, au moins une fois par semestre. Deuxièmement, la loi a institué la commission G10, qui doit autoriser les mesures de surveillance et possède des pouvoirs importants à tous les stades de l'interception. La Cour observe que, dans son arrêt *Klass e.a.*, elle a estimé que ce système de supervision – qui était essentiellement le même que celui prévu par la loi G10 dans sa teneur modifiée en litige en l'espèce – était apte à limiter à ce qui était « nécessaire, dans une société démocratique » l'ingérence résultant de la législation incriminée. Elle ne voit aucune raison de conclure différemment en l'espèce »[42].

Comme on le constate, le mécanisme de contrôle, bien que non judiciaire, est considéré comme suffisant par la Cour, principalement par référence à l'analyse réalisée dans l'arrêt *Klass c. Allemagne*[43]. Cette validation par simple renvoi à une décision prononcée près de trente ans plus tôt révèle à nouveau l'absence de prise en considération par la Cour européenne des droits de l'homme des évolutions technologiques enregistrées depuis lors. En 1978, la loi allemande ne concernait que l'interception du courrier postal et des télécommunications

[42] Cour eur. dr. h., décision *Weber et Saravia c. Allemagne*, précité, § 117.
[43] Cour eur. dr. h., arrêt *Klass e.a. c. Allemagne*, précité, §§ 65-72.

fixes, visant uniquement les personnes suspectes d'infractions graves ou les personnes présumées avoir des contacts avec elles. Dans l'affaire *Weber et Saravia*, il s'agissait d'une surveillance stratégique susceptible d'impliquer l'interception des télécommunications mobiles de toute personne, à l'étranger[44]. La Cour n'a donc pas estimé nécessaire d'adapter son analyse des garanties procédurales à l'extension de la portée des mesures de surveillance.

L'effectivité de tout mécanisme de contrôle soulève encore le problème de l'existence d'une procédure de notification, permettant aux personnes placées sous surveillance de prendre connaissance des mesures dont elles ont fait l'objet et d'exercer le cas échéant des recours si elles estiment avoir été victimes de pratiques abusives. Dans sa jurisprudence, la Cour européenne des droits de l'homme a considéré que l'absence de notification ne rendait pas nécessairement l'ingérence dans la vie privée non nécessaire, mais qu'une telle notification était néanmoins « souhaitable » :

> « La Cour rappelle que la question de la notification ultérieure de mesures de surveillance est indissolublement liée au caractère effectif des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance ; si on ne l'avise pas des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice. Toutefois, l'absence de notification ultérieure aux personnes touchées par des mesures de surveillance secrète, dès la levée de celles-ci, ne saurait en soi justifier la conclusion que l'ingérence n'était pas 'nécessaire, dans une société démocratique', car c'est précisément cette absence d'information qui assure l'efficacité de la mesure constitutive de l'ingérence. En effet, pareille notification risquerait de révéler les méthodes de travail des services de renseignements et leurs champs d'observation. Cependant, il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction. »[45]

Dans les affaires *Klass c. Allemagne* et *Weber et Saravia*, la Cour avait conclu que l'attribution à une autorité indépendante du pouvoir de décider si une notification *a posteriori* se justifiait ou non, était suffisante pour offrir aux individus les garanties nécessaires. La Cour a également jugé qu'une absence totale de système de notification pouvait rester compatible avec les exigences de la Convention, lorsque les personnes concernées avaient la possibilité de

[44] Dans l'arrêt *Klass c. Allemagne*, la Cour avait d'ailleurs souligné qu'en l'espèce « la législation incriminée n'autorise pas une surveillance dite exploratoire ou générale » (§ 51). Une remarque similaire avait été faite dans l'affaire *Kennedy c. Royaume-Uni* (arrêt du 18 mai 2010, § 160).

[45] Cour eur. dr. h., décision *Weber et Saravia c. Allemagne*, précité, § 135 (références omises).

saisir un organe de contrôle sur la simple base de soupçons du fait que ses communications faisaient ou avaient fait l'objet d'interceptions, sans que la compétence de cet organe ne soit subordonnée à une notification de l'interception[46].

Au final, la jurisprudence traditionnelle de la Cour européenne des droits de l'homme s'est avérée assez peu exigeante dans son contrôle des régimes de surveillance, reconnaissant aux États une « ample marge d'appréciation » quant à la définition du choix des mesures, et se refusant à prendre en considération les caractéristiques propres de la surveillance non ciblée, et à en répercuter les spécificités dans son analyse des critères de proportionnalité.

Dans le point suivant, nous montrerons que cette position a été remise en cause par les instances des droits de l'homme de l'ONU et par la Cour de justice, à la suite de la prise de conscience des conséquences potentielles de la surveillance de masse, compte tenu des informations révélées sur les programmes d'espionnage des services de renseignement des États-Unis.

II. Les travaux des rapporteurs spéciaux des Nations Unies et la jurisprudence de la Cour de justice de l'Union européenne : l'exigence d'une « stricte nécessité »

Après les révélations concernant les programmes de renseignement menés par la National Security Agency (NSA) et la probable implication de services de sécurité européens dans leur mise en œuvre, diverses instances régionales et internationales ont porté leur attention sur les implications des mesures de surveillance sur le respect des droits fondamentaux. Outre l'adoption en 2013 et 2014 de résolutions par l'Assemblée générale des Nations Unies portant sur le « droit à la vie privée à l'ère du numérique », déjà mentionnées, on peut citer plusieurs résolutions du Parlement européen[47] et du Comité des ministres du Conseil de l'Europe[48].

[46] Cour eur. dr. h., arrêt *Kennedy c. Royaume-Uni*, précité, § 167.

[47] Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'Agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, P7_TA-PROV(2013)0322 ; résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, P7_TA(2014)0230.

[48] Déclaration du Comité des ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux, adoptée le 11 juin 2013, lors de la 1173e réunion des délégués des ministres.

De manière plus précise, tant la Cour de justice de l'Union européenne (A) que les instances de l'ONU en matière de droits de l'homme (B) ont eu l'occasion de se prononcer sur les conditions de conformité aux droits de l'homme des pratiques de traitement massif de données à des fins de surveillance. À cet égard, elles ont adopté une position qui s'écarte de la voie suivie classiquement par la Cour européenne des droits de l'homme, en se montrant plus exigeantes quant à l'analyse de la proportionnalité de la mesure, lorsque celle-ci présente un caractère non ciblé.

A. *La jurisprudence de la Cour de justice de l'Union européenne en matière de protection des données personnelles*

Dans l'affaire *Digital Rights Ireland*, la Cour de justice de l'Union européenne était saisie de plusieurs questions préjudicielles portant sur la validité de la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications[49]. La question soulevée consistait principalement à déterminer si l'obligation faite aux opérateurs de télécommunications de conserver les données de communications électroniques pendant une durée minimale de six mois, afin d'en permettre la disponibilité en cas d'enquête sur des infractions graves, était compatible avec les droits fondamentaux des individus. Dans son raisonnement, la Cour a donné une large place à l'analyse de la portée technologique de la mesure concernée. Elle a ainsi observé que « la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves ». Le caractère non ciblé de l'obligation de conservation des données de communication constitue de ce fait un élément qui influe directement sur l'évaluation de la proportionnalité :

> « D'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur

[49] C.J.U.E., Gde Ch., arrêt *Digital Rights Ireland Ltd (C-293/12)*, précité, 8 avril 2014.

comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves. »[50]

Le caractère indiscriminé et très général de la collecte et du traitement de données personnelles, fût-il dans l'objectif de la répression et la prévention d'infractions graves, est donc aux yeux de la Cour un élément permettant de caractériser la disproportion du système au regard de l'objectif poursuivi, entraînant ainsi un constat d'illégalité de la directive concernée. Plus la surveillance couvre un nombre important d'individus et traite de manière massive les données, plus la proportionnalité est analysée avec rigueur et s'avère difficile à établir. À l'« ample marge d'appréciation de l'État » admise par la Cour européenne des droits de l'homme, la Cour de justice a substitué le « pouvoir d'appréciation réduit »[51], impliquant la nécessité d'un « contrôle strict »[52] de l'ingérence dans les droits fondamentaux, qui doit s'opérer « dans les limites du strict nécessaire »[53]. Dans l'affaire *Digital Rights*, la Cour a ainsi énoncé :

« En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

[…]

[50] *Ibid.*, §§ 58-59.
[51] *Ibid.*, § 48.
[52] *Ibid.*
[53] *Ibid.*, § 52.

> S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire »[54].

Cette approche a été confirmée par la Cour de justice dans l'affaire *Maximillian Schrems c. Data Protection Commissioner*[55], qui soulevait la question de la légalité du transfert vers les États-Unis de données personnelles issues d'un compte Facebook, transfert autorisé par la Commission européenne en vertu d'une décision reconnaissant que cet État assure un niveau adéquat de protection. Dans son évaluation de la légalité de la décision de la Commission, la Cour a, de nouveau, pris en considération l'étendue des personnes visées et la portée des traitements dont leurs données seraient susceptibles d'être l'objet. La Cour a ainsi considéré que la nécessité d'offrir des garanties suffisantes contre les abus était d'autant plus cruciale que ces données « sont soumises à un traitement automatique »[56] et qu'est prévue la conservation « généralisée […] de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées »[57]. Il s'ensuit qu'une « réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée »[58]. Le traitement massif d'informations concernant un nombre élevé de personnes apparaît dès lors, en l'absence de règles précises et de garanties suffisantes, constituer une violation du droit à la vie privée, même dans l'objectif de la protection de la sécurité nationale[59].

---

[54] *Ibid.*, §§ 48 et 52.

[55] C.J.U.E., Gde Ch., arrêt *Maximillian Schrems c. Data Protection Commissioner*, précité, en particulier les paragraphes 78 et 92.

[56] *Ibid.*, § 91.

[57] *Ibid.*, § 93.

[58] *Ibid.*, § 94.

[59] Sur ces deux arrêts, voy. notamment J.-P. Foegle, « Chronique du droit 'post-Snowden' : la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme*, http://revdh.revues.org/2074.

B. *Les travaux des instances de l'ONU en matière de droits de l'homme*

Les instances de l'ONU en matière de droits de l'homme ont également largement souligné l'impact des technologies numériques sur la portée des mesures de surveillance, et le besoin de tenir compte de cette portée dans l'analyse du critère de proportionnalité[60]. Le rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a ainsi mis en évidence le changement de paradigme impliqué par l'émergence de la surveillance de masse :

> « Les États ayant des taux de pénétration de l'internet élevés peuvent ainsi avoir accès au contenu des appels téléphoniques et des courriels d'un nombre effectivement illimité d'utilisateurs et garder un aperçu des activités sur la Toile associées à des sites web particuliers. Tout ceci est possible sans soupçon préalable concernant une personne ou une organisation spécifique. Les communications de chaque utilisateur d'internet sont pour ainsi dire potentiellement ouvertes à l'inspection des services de renseignement et des organismes d'application de la loi des États concernés. Ceci équivaut à une immixtion systématique dans le droit au respect du secret des communications et exige une justification obligatoire correspondante. »[61]

Le rapporteur spécial en conclut qu'il est très douteux qu'un tel mode de récolte de renseignements puisse satisfaire de manière convaincante au critère de proportionnalité :

> « La capacité technique de réaliser de vastes programmes de collecte et d'analyse de données offre indéniablement un moyen de plus pour lutter contre le terrorisme et mener des enquêtes sur l'application de la loi. Mais une évaluation de la proportionnalité de ces programmes doit également prendre en considération les dommages collatéraux causés aux droits collectifs à la vie privée. Les programmes de collecte de grandes quantités de données semblent porter atteinte à la prescription selon laquelle les services de renseignement doivent choisir la mesure la moins intrusive possible pour les droits de l'homme (à moins que les États concernés ne soient à même de dé-

[60] Voy. le rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, 17 avril 2013, A/HRC.23/40, pp. 4-6 ; rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit à la vie privée à l'ère du numérique », A/HRC/27/37, 30 juin 2014, pp. 3-4.

[61] Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, A/69/397, 23 septembre 2014, § 9.

> montrer que rien d'autre qu'un accès global à toutes les communications sur internet ne peut suffire pour assurer une protection contre les menaces terroristes et autres délits graves). Puisqu'il n'est pas possible d'entreprendre une évaluation personnalisée de la proportionnalité avant de recourir à de telles mesures, ces programmes semblent aussi mettre en cause l'essence même du droit à la vie privée. Ils excluent purement et simplement l'analyse « au cas par cas » jugée essentielle par le Comité des droits de l'homme et ils peuvent donc être jugés arbitraires, même s'ils servent un objectif légitime et ont été adoptés sur la base d'un régime juridique accessible. En conséquence, le rapporteur spécial arrive à la conclusion que de tels programmes ne peuvent être compatibles avec l'article 17 du Pacte que si les États concernés sont en mesure de justifier la proportionnalité de l'immixtion systématique dans les droits à la vie privée sur l'internet d'un nombre potentiellement illimité de personnes innocentes n'importe où dans le monde. »[62]

Concernant l'existence de garanties procédurales permettant de s'assurer du respect des droits fondamentaux dans la mise en œuvre des activités de renseignement, le rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste s'est à nouveau montré plus strict que la Cour européenne des droits de l'homme qui, comme nous l'avons vu, n'avait pas estimé que les mesures de surveillance non ciblées appelaient des garanties procédurales spécifiques. En effet, le rapporteur a pointé les difficultés particulières posées à ce sujet par la surveillance de masse :

> « Dans le contexte de la surveillance ciblée, quelle que soit la méthode d'autorisation préalable adoptée (par le judiciaire ou l'exécutif), il existe au moins une possibilité d'examen *ex ante* de la nécessité et de la proportionnalité d'une mesure de surveillance intrusive par rapport aux circonstances particulières du cas et à la personne ou l'organisation dont les communications doivent être interceptées. Aucune de ces possibilités n'existe dans le contexte des systèmes de surveillance de masse puisqu'ils ne sont pas fondés sur le soupçon individuel. L'examen *ex ante* se limite ainsi à autoriser l'application du système dans son ensemble plutôt qu'à une personne déterminée. Le rapporteur spécial estime que les États qui ont recours aux technologies de surveillance de masse doivent mettre en place des organes de contrôle tout à fait indépendants, disposant de ressources suffisantes et chargés de procéder à l'examen préalable de l'emploi de techniques de surveillance intrusive

[62] Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, § 52.

> par rapport aux exigences de l'article 17 du Pacte [international relatif aux droits civils et politiques] concernant les critères de légalité, de nécessité et de proportionnalité. »[63]

Il est donc nécessaire que l'organe de contrôle puisse exercer une analyse spécifique de la proportionnalité de la décision de procéder à une surveillance non ciblée, au regard de l'exigence de nécessité. Le régime de surveillance doit également prévoir un recours *a posteriori* dans le cadre d'un « mécanisme indépendant capable de réaliser un examen approfondi et impartial, ayant accès à toute la documentation pertinente et donnant des garanties d'application régulière de la loi »[64]. Concernant l'accès à ce mécanisme pour les régimes de surveillance de masse, le rapporteur spécial « considère que tout utilisateur d'internet devrait avoir le droit de contester la légalité, la nécessité et la proportionnalité des mesures en cause »[65].

On constate ainsi que la jurisprudence de la Cour de justice de l'Union européenne et les travaux des rapporteurs spéciaux des Nations Unies ont adopté une approche spécifique concernant les techniques de surveillance non ciblée, en posant pour ce type de techniques l'exigence d'un contrôle de proportionnalité strict, ne reconnaissant à l'État qu'un pouvoir d'appréciation réduit et appelant à l'établissement de garanties procédurales adaptées. Pour la première fois depuis les révélations d'Edward Snowden, la Cour européenne des droits de l'homme avait l'occasion de se pencher sur la question de la surveillance de masse, en se prononçant dans les affaires *Roman Zakharov c. Russie* et *Szabó et Vissy c. Hongrie*.

---

[63] Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, § 47.

[64] *Ibid.*, § 49. Voy. également United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, « Joint Declaration on surveillance programs and their impact on freedom of expression », 21 juin 2013, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1 ; rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit à la vie privée à l'ère du numérique », *op. cit.*, §§ 37-38.

[65] Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, § 50. Voy. également rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit à la vie privée à l'ère du numérique », *op. cit.*, §§ 39-41.

III. Les arrêts *Roman Zakharov c. Russie* et *Szabó et Vissy c. Hongrie* : des réponses divergentes concernant la surveillance de masse

Les situations soumises à la Cour européenne des droits de l'homme dans les affaires *Roman Zakharov c. Russie* et *Szabó et Vissy c. Hongrie* étaient assez similaires[66]. Dans les deux cas, la requête était introduite par les membres d'ONG actives dans le domaine des droits humains et mettait en cause le régime législatif existant en matière de surveillance, autorisant l'adoption par les services de renseignement de mesures considérées comme étant susceptibles de porter atteinte au droit à la vie privée des requérants (article 8 de la Convention). Comme dans d'autres affaires, c'est donc à une évaluation globale du régime de surveillance que la Cour devait procéder. Dans les deux affaires, les législations concernées permettaient l'adoption de mesures d'interception des communications à l'égard de personnes qui n'étaient pas soupçonnées d'avoir commis une infraction pénale. La loi russe, pour des « faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Fédération de Russie » ou encore pour obtenir « des informations pertinentes pour le dossier relatif à une infraction pénale de gravité moyenne, une infraction grave ou une infraction pénale particulièrement grave »[67]. La loi hongroise, pour « prévenir les actes terroristes, ou dans l'intérêt de la sécurité nationale de la Hongrie » ou « dans le but de secourir les citoyens hongrois capturés à l'étranger dans des zones de guerre ou dans le cadre d'actes de terrorisme »[68]. Ce caractère potentiellement non ciblé des mesures de surveillance concernées obligeait la Cour à se positionner sur deux types de questions. Tout d'abord, elle devait clarifier la question de la recevabilité de la requête introduite par des personnes n'ayant pas démontré qu'elles avaient effectivement fait l'objet de mesures d'interception de leurs communications (A). Ensuite, elle devait déterminer s'il était nécessaire d'ajuster les critères de proportionnalité en cas de surveillance susceptible de prendre une portée non ciblée (B). Dans quelle mesure, à travers ces questions, la Cour allait-elle tenir compte de la spécificité de la surveillance de masse et prendre en considération l'évolution marquée par les arrêts de la Cour de justice de l'Union européenne et les rapports de l'ONU ? Comme nous le verrons, les approches à cet égard ont été divergentes dans les deux décisions, dont l'une a été rendue par la Grande Chambre de la Cour.

[66] Sur ces affaires, voy. aussi J.-P. Foegle, *op. cit.*

[67] Cour eur. dr. h., Gde Ch., arrêt *Roman Zakharov c. Russie*, 4 décembre 2015, §§ 31 et 32.

[68] Cour eur. dr. h., arrêt *Szabó et Vissy c. Hongrie*, 12 janvier 2016, § 11.

A. *La qualité de « victime »*

Dans l'affaire *Roman Zakharov*, le gouvernement russe contestait la recevabilité de la requête, en arguant du fait qu'il n'était pas établi que les requérants avaient effectivement fait l'objet d'une mesure d'interception de leurs communications par les services de renseignement[69]. Joignant cette question au fond dans l'examen du constat de l'existence d'une « ingérence », la Cour a jugé nécessaire de « préciser les conditions dans lesquelles un requérant peut se prétendre victime d'une violation de l'article 8 [de la Convention] sans avoir à démontrer que des mesures de surveillance secrète lui ont bien été appliquées, de manière à permettre l'adoption d'une approche uniforme et prévisible »[70]. Se référant plus particulièrement à l'affaire *Kennedy c. Royaume-Uni*[71], la Cour a admis qu'un requérant puisse se prétendre victime d'une violation entraînée par la simple existence de mesures de surveillance secrète aux conditions suivantes :

> « Premièrement, la Cour prendra en considération la portée de la législation autorisant les mesures de surveillance secrète et recherchera pour cela si le requérant peut éventuellement être touché par la législation litigieuse, soit parce qu'il appartient à un groupe de personnes visées par elle, soit parce qu'elle concerne directement l'ensemble des usagers des services de communication en instaurant un système dans lequel tout un chacun peut voir intercepter ses communications. Deuxièmement, la Cour tiendra compte de la disponibilité de recours au niveau national et ajustera le niveau de son contrôle en fonction de l'effectivité de ces recours »[72].

Concernant cette deuxième condition, la Cour a expliqué que « lorsque l'ordre interne n'offre pas de recours effectif à la personne qui pense avoir fait l'objet d'une surveillance secrète […], on est fondé à alléguer que la menace de surveillance restreint par elle-même la liberté de communiquer au moyen des services des postes et télécommunications et constitue donc, pour chaque usager ou usager virtuel, une atteinte directe au droit garanti par l'article 8 »[73]. Dans un tel cas de figure, « un contrôle accru par la Cour s'avère donc nécessaire et il se justifie de déroger à la règle selon laquelle les particuliers n'ont pas le droit de se plaindre d'une loi *in abstracto* »[74]. Par contre, lorsqu'il existe

[69] Cour eur. dr. h., Gde Ch., arrêt *Roman Zakharov c. Russie*, précité, §§ 152 et s.
[70] *Ibid.*, § 170.
[71] Cour eur. dr. h., arrêt *Kennedy c. Royaume-Uni*, précité.
[72] *Ibid.*, § 171.
[73] *Ibid.*
[74] *Ibid.*

un recours effectif sur le plan national, la Cour indique que l'intéressé ne pourra se prétendre victime que « s'il est à même de montrer qu'en raison de sa situation personnelle il est potentiellement exposé au risque de subir pareilles mesures »[75]. En l'espèce, la Cour relève que « la législation incriminée a instauré un système de surveillance secrète dans le cadre duquel tout usager de services de téléphonie mobile proposés par des fournisseurs russes peut voir intercepter ses communications de téléphonie mobile, sans jamais être informé de cette surveillance »[76]. Dès lors que « le droit russe n'offre pas de recours effectifs à une personne qui pense avoir fait l'objet d'une surveillance secrète », la Cour en conclut que « le requérant est en droit de se prétendre victime d'une violation de la Convention bien qu'il ne puisse alléguer à l'appui de sa requête avoir fait l'objet d'une mesure concrète de surveillance »[77].

Une position similaire est adoptée par la chambre dans l'affaire *Szabó et Vissy*, qui constate que « the legislation directly affects all users of communication systems and all homes » et que « the domestic law does not appear to provide any possibility for an individual who alleges interception of his or her communications to lodge a complaint with an independent body »[78].

On remarque ainsi que le caractère potentiellement massif de la surveillance, au même titre que son caractère secret, est pris en considération par la Cour pour élargir le critère de recevabilité généralement retenu, et admettre la qualité de « victime » et l'existence d'une « ingérence » même en l'absence de mesure précise de surveillance subie par le requérant. On reste cependant perplexe sur la pertinence du lien intrinsèque établi par la Cour entre l'effet potentiel du régime de surveillance sur tout citoyen et l'existence d'un recours effectif au plan national, le second élément étant considéré comme étant de nature à contrebalancer le premier dans l'analyse de la recevabilité de la requête. Les deux décisions de la Cour ayant conclu à l'absence de recours effectif, il n'est guère aisé de savoir dans quelle mesure l'existence d'un tel recours permettrait d'écarter *ipso facto* la qualité de victime et l'existence de l'ingérence. En effet, dans le cas d'un régime de surveillance secret et non ciblé, la seule existence d'un recours effectif ne permet pas de garantir, comme on le verra, la proportionnalité du système. La potentialité pour une personne de faire l'objet, à son insu, d'une mesure d'interception, devrait l'obliger à introduire des recours à intervalles réguliers pour s'assurer qu'elle n'a pas effectivement été l'objet d'une telle mesure. Ceci montre que c'est la nature « non ciblée et secrète » du

[75] *Ibid.*
[76] *Ibid.*, § 175.
[77] *Ibid.*, §§ 176 et 179.
[78] Cour eur. dr. h., arrêt *Szabó et Vissy c. Hongrie*, précité, §§ 38-39.

système de surveillance qui, à elle seule, implique la qualité de victime et l'ingérence, indépendamment de l'existence d'un recours effectif, qui ne constitue que l'un des éléments permettant d'évaluer, au fond, la proportionnalité du régime.

B. *L'analyse de la proportionnalité*

Concernant l'examen de la proportionnalité des régimes russe et hongrois de surveillance, il était intéressant de voir si la Cour européenne des droits de l'homme allait faire évoluer sa jurisprudence, en tenant compte à la fois de la prise de conscience des effets potentiels considérables de la surveillance de masse, après les révélations faites concernant les programmes de la National Security Agency (NSA), et de l'affirmation du besoin de critères d'analyse spécifiques pour évaluer ce type de surveillance, émanant tant des instances de l'ONU que de la Cour de justice de l'Union. Dans l'affaire *Roman Zakharov c. Russie*, le requérant « alléguait que le système d'interception secrète des communications de téléphonie mobile en Russie avait emporté violation de son droit au respect de sa vie privée et de sa correspondance et qu'il n'avait pas disposé d'un recours effectif permettant de s'en plaindre »[79]. Dans l'examen de ce recours, la Grande Chambre a réitéré le principe selon lequel « les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale »[80]. En l'occurrence, elle n'a ainsi pas estimé que le fait que le système de surveillance concerné par le recours soit susceptible de viser « une personne non soupçonnée d'une infraction » appelait un traitement particulier, en raison du caractère stratégique ou indifférencié de la surveillance. Conformément à sa jurisprudence traditionnelle, la Cour a dès lors centré son analyse sur la précision de la loi et l'existence de garanties procédurales[81], au regard des aspects déjà identifiés dans ses jurisprudences antérieures :

> « La Cour appréciera donc successivement l'accessibilité du droit interne, la portée et la durée des mesures de surveillance secrète, les procédures à

[79] Cour eur. dr. h., Gde Ch., arrêt *Roman Zakharov c. Russie*, précité, § 3.

[80] *Ibid.*, § 232.

[81] Il faut préciser que la Cour a choisi d'examiner conjointement les critères de légalité et de proportionnalité, sans les distinguer dans son raisonnement : « La 'qualité de la loi' en ce sens implique que le droit interne doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont 'nécessaires dans une société démocratique', notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus » (§ 236).

suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées, les procédures d'autorisation, les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne. »[82]

Et c'est en analysant la législation russe au regard de ces divers éléments que la Cour a abouti au constat d'une violation de l'article 8 de la Convention :

« La Cour déduit de ce qui précède que les recours évoqués par le gouvernement sont ouverts uniquement aux personnes qui disposent d'informations relatives à l'interception de leurs communications. L'effectivité de ces recours est donc compromise par l'absence d'obligation de donner notification à un stade quelconque à la personne visée par l'interception, et par l'inexistence d'une possibilité satisfaisante de demander et d'obtenir auprès des autorités des informations sur les interceptions. La Cour estime en conséquence que le droit russe n'offre pas de recours judiciaire effectif contre les mesures de surveillance secrète dans les cas où une procédure pénale n'a pas été engagée contre le sujet de l'interception »[83].

C'est donc au regard d'une appréciation classique du critère de proportionnalité que la Grande Chambre a conclu que le système légal russe de surveillance n'offrait pas toutes les garanties nécessaires contre les possibilités d'abus, au terme d'une appréciation globale du régime juridique, en mettant l'accent principalement sur l'insuffisance des recours face au flou de certaines dispositions[84]. Comme dans sa jurisprudence précédente, la Cour n'a guère accordé d'attention à la portée plus ou moins générale des mesures de surveillance concernées, se limitant à nouveau à s'en tenir à leur caractère « secret », seul facteur essentiel à ce stade du raisonnement pour évaluer la proportionnalité du régime de renseignement. Tout en relevant, ici ou là[85], les ambiguïtés de la loi et de la pratique russes quant à l'étendue des personnes susceptibles de faire l'objet d'une mesure de surveillance, jamais la Cour n'a caractérisé avec précision cette portée ni, *a fortiori*, n'en a tiré des conséquences précises sur la méthode d'évaluation de la proportionnalité. La Cour n'a donc pas pris en considération la nature intrinsèque des mesures autorisées et leur nécessité au regard de l'objectif de protection de la « sécurité nationale, militaire, écono-

[82] *Ibid.*, § 238.
[83] *Ibid.*, § 298.
[84] *Ibid.*, §§ 235 et s.
[85] Voy. notamment les §§ 245-249.

mique ou écologique» de la Fédération de Russie, mais a limité son examen à la vérification de l'existence «des garanties et des garde-fous suffisants»[86].

Ce mode de raisonnement a été remis en cause, quelques jours plus tard, par l'arrêt rendu dans l'affaire *Szabó et Vissy c. Hongrie*. Une chambre de la Cour a cette fois développé une analyse qui prend pleinement en considération les spécificités de la surveillance à grande échelle, aux fins d'évaluation du critère de proportionnalité pour la soumettre à des critères de compatibilité avec l'article 8 de la Convention plus stricts:

> «[I]n the present case, the Court considers that, in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern.
>
> The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament. This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention.»[87]

Cela conduit la Cour à adopter le test de la «stricte nécessité» tel qu'il avait été formulé par la Cour de justice et le rapporteur spécial de l'ONU, dès lors que l'on se trouve confronté à une surveillance de masse[88]. La chambre a explicité la portée de ce contrôle plus étroit de la manière suivante:

> «However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement 'necessary in a democratic society' must be interpreted in this context as requiring 'strict necessity' in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these cri-

[86] *Ibid.*, § 237.
[87] Cour eur. dr. h., *Szabó et Vissy c. Hongrie*, précité, §§ 69-70.
[88] *Ibid.*, § 73.

teria will be prone to abuse by the authorities with formidable technologies at their disposal. »[89]

Le contrôle de stricte nécessité doit donc s'envisager en deux étapes. La première vise à évaluer la proportionnalité de la mesure de surveillance dans sa nature, compte tenu de sa portée et de ses caractéristiques technologiques. Si une mesure de surveillance présente un caractère non ciblé, l'État devra être à même de justifier en quoi une telle méthode est nécessaire à la préservation de la sécurité nationale, sans se prévaloir de la « large marge d'appréciation » que la jurisprudence traditionnelle de la Cour lui accorde à cet égard. Comme le soulignait le rapporteur spécial des Nations Unies, cela impliquerait de pouvoir démontrer que seule une collecte massive de données permette d'assurer une protection contre les menaces terroristes[90]. Si ce premier test est franchi, il faudra encore vérifier que, dans le cadre d'une opération spécifique, le choix de recourir à ce type de mesures se justifie pour recueillir des informations essentielles à la préservation de la sécurité nationale, à l'exclusion de voies alternatives moins intrusives (une surveillance plus ciblée, par exemple). En l'espèce, la Cour a accordé une attention particulière à l'analyse de la portée potentielle des mesures de surveillance, susceptible de viser des personnes qui ne sont pas soupçonnées d'activités terroristes :

« It is of serious concern, however, that the notion of 'persons concerned identified … as a range of persons' might include indeed any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens. The Court notes the absence of any clarification in domestic legislation as to how this notion is to be applied in practice. For the Court, the category is overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons 'concerned' and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity with regard to the aims pursued and the means employed. »[91]

Cette circonstance particulière, combinée au manque d'encadrement légal et procédural caractérisant le système hongrois de surveillance, a dès lors fourni

[89] *Ibid.*

[90] Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, § 52.

[91] *Ibid.*, § 67.

à la Cour l'un des motifs principaux du constat de violation de l'article 8 de la Convention par la Hongrie :

> « Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention. »[92]

La décision de la chambre marque ainsi un certain tournant dans la jurisprudence de la Cour européenne des droits de l'homme, puisqu'un moyen de surveillance non ciblée doit en lui-même satisfaire le critère de stricte nécessité. Cela signifie que dans le choix des méthodes de surveillance inscrites dans sa loi, l'État ne dispose plus de sa « large marge d'appréciation », mais doit pouvoir expliquer qu'un dispositif de surveillance susceptible de prendre une dimension massive est « strictement nécessaire » à la défense de la sécurité nationale. Cette justification doit porter sur la nature même des mesures de surveillance, indépendamment du fait de savoir si elles sont encadrées de manière suffisamment précise par des critères légaux et des recours suffisants. Ces derniers éléments ne sont à évaluer que dans un second temps, et ils devront l'être d'autant plus strictement que la surveillance est susceptible de concerner un groupe important de personnes, non suspectées d'activités mettant en péril la sécurité nationale. Le critère de stricte nécessité interviendra donc tant pour apprécier la légalité de la mesure en son principe qu'au regard des « garde-fous » qui l'entourent.

Il s'agit là d'une importante évolution de jurisprudence, qui rejoint la voie tracée par la Cour de justice de l'Union européenne et les instances de l'ONU. Elle a fait l'objet de certaines critiques exprimées par l'un des juges dans une opinion séparée. Toutefois, ces critiques paraissent fondées sur une mauvaise compréhension de la portée de l'analyse opérée par la chambre. De manière quelque peu paradoxale, le juge Pinto de Albuquerque reproche à la chambre d'avoir, d'une certaine manière, légitimé le recours à la surveillance de masse, en lui appliquant des critères distincts de ceux définis traditionnellement par la jurisprudence de la Cour pour tous types de mesures de surveillance[93]. Ce reproche nous paraît mal fondé. En effet, il part du présupposé erroné que les

[92] *Ibid.*, § 89.

[93] Cour eur. dr. h., arrêt *Szabó et Vissy c. Hongrie*, précité, opinion concordante du juge Pinto de Albuquerque, § 20.

mesures de surveillance non ciblées auraient, dans la jurisprudence antérieure de la Cour, été par principe invalidées sur la base de l'examen traditionnel de proportionnalité, et que seules seraient dès lors admises les mesures visant des personnes sur lesquelles pèseraient des « soupçons raisonnables » de commission, passée ou future, d'infractions ou d'atteinte à la sécurité nationale. C'est donc à mauvais escient que le juge de Albuquerque renvoie à l'affaire *Weber et Saravia c. Allemagne*[94], puisque dans ce cas le système allemand autorisait bien une « surveillance stratégique générale », sans que cet élément n'ait entraîné un quelconque constat de violation. Ce qu'a en réalité fait la Chambre dans son arrêt *Szabó et Vissy c. Hongrie*, c'est identifier de manière particulière la pratique de plus en plus répandue de l'utilisation de la surveillance de masse par les services de renseignements européens et de la soumettre à un critère de nécessité autonome et plus exigeant[95], en raison des risques plus importants qu'elle comporte pour le respect de la vie privée de personnes sur lesquelles ne pèse pas de « soupçon individuel »[96].

En définitive, il nous apparaît que la décision rendue par la Cour dans l'affaire *Szabó et Vissy c. Hongrie*, à l'instar de la Cour de justice de l'Union européenne ou des instances de l'ONU, est partie du constat concret que la lutte contre le terrorisme entraîne de plus en plus la mise en place de techniques de surveillance de masse et que, sauf à les déclarer illégales en leur principe, ce qu'aucun texte international ne permet de faire, leur encadrement effectif doit passer par la définition d'un critère de proportionnalité très exigeant, qui s'applique non seulement aux garanties légales qui l'accompagnent, mais également au principe même de la mesure concernée. Il reste à savoir si cette approche est appelée à être confirmée par des décisions ultérieures de la Cour européenne des droits de l'homme, en particulier dans le chef de la Grande Chambre.

---

[94] *Ibid.*, § 20, note 36.

[95] C'est ce raisonnement que ne comprend pas le juge lorsqu'il croit voir une contradiction entre l'adoption du critère de « stricte nécessité » pour la surveillance non ciblée et le constat par la Cour que des systèmes de surveillance sont mis en place en vue de procéder au traitement de données concernant des personnes sur lesquelles ne pèsent pas de soupçon individuel : « It is logically inconsistent that the same judgment imposes a 'strict necessity' test for the determination of the surveillance measure, but at the same time accepts a very loose criterion for the degree of suspicion of involvement in the offences or activities being monitored, as demonstrated above. It is logically incoherent to criticise the overly broad text of the Hungarian law when it refers to the 'persons concerned identified as a range of persons' and yet to accept the linguistically vague and legally imprecise 'individual suspicion' test to ground the applicability of a surveillance measure. » (opinion concordante du juge Pinto de Albuquerque, § 21).

[96] Cour eur. dr. h., arrêt *Szabó et Vissy c. Hongrie*, précité, § 71.

Conclusions

Le changement de paradigme entraîné par les développements technologiques permettant la mise en place d'une surveillance de masse a posé avec acuité la question de la manière dont le respect des droits de l'homme doit être assuré dans la mise en place de telles méthodes. Ce débat n'est pas prêt de s'éteindre, puisqu'on constate un mouvement législatif au sein des États européens allant dans le sens d'accroître les pouvoirs des services de renseignement et d'autoriser des techniques de surveillance à grande échelle, comme l'illustre l'adoption par la France de la loi sur le renseignement en juillet 2015[97] ou le projet britannique « Investigatory Powers Bill », déposé à la Chambre des Communes en mars 2016[98]. Ces législations et d'autres pratiques de services de renseignements européens ont suscité de vives inquiétudes jusqu'au sein du Parlement européen[99] et de l'Assemblée parlementaire du Conseil de l'Europe[100], qui ont mis en garde contre les dangers des opérations de surveillance massive.

Dans les deux affaires commentées, la Cour avait l'occasion de préciser la façon dont sa jurisprudence devait s'appliquer à la situation de la surveillance non ciblée. Comme nous l'avons vu, les décisions rendues ont été dans une certaine mesure divergentes et n'ont pas permis d'éclaircir complètement la situation. La décision de la chambre dans l'affaire *Szabó et Vissy c. Hongrie* a eu le mérite d'aborder la problématique de la surveillance de masse de manière spécifique, ce qui obligera la Cour – et le cas échéant la Grande Chambre – à se positionner de manière précise dans sa jurisprudence ultérieure. L'opportunité devrait lui en être donnée bientôt, puisque plusieurs affaires pendantes visent

[97] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *J.O.R.F.* n° 0171 du 26 juillet 2015, p. 12735.

[98] Investigatory Powers Bill 2015-16, http://services.parliament.uk/bills/2015-16/investigatorypowers.html.

[99] Résolution du Parlement européen du 29 octobre 2015 sur le suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne, P8_TA-PROV(2015)0388.

[100] Assemblée parlementaire du Conseil de l'Europe, « Les opérations de surveillance massive », rapport rédigé par M. Pieter Omtzigt, Commission des questions juridiques et des droits de l'homme, 18 mars 2015, Doc. 13734; Assemblée parlementaire du Conseil de l'Europe, résolution 2045 (2015), 21 avril 2015. Voy. également Council of Europe, European Commission for Democracy through Law (Venice Commission), « Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies », 7 avril 2015, étude n° 719/2013, CDL-AD(2015)006.

la législation britannique[101], tandis que la loi française a fait l'objet de treize requêtes distinctes[102].

☆

Le site internet de la *revue* propose à ses lecteurs un dossier permettant d'accéder rapidement aux principaux actes et documents renseignés dans l'article qui précède (www.rtdh.eu, onglet « Sommaires », « n° 108 octobre 2016 », cliquer ensuite sur le titre de l'article).

[101] *Big Brother Watch e.a. c. Royaume-Uni*, 58170/13 ; *Bureau of Investigative Journalism and Alice Ross c. Royaume-Uni*, 62322/14 ; *10 human-rights organisations c. Royaume-Uni*, 24960/15.

[102] *Association confraternelle de la presse judiciaire e.a. c. France*, 49526/15 ; *Martin c. France*, 49616/15 ; *Lecomte c. France*, 49615/15 ; *Babonneau c. France*, 49617/15 ; *Souchard c. France*, 49618/15 ; *Triomphe c. France*, 49619/15 ; *Egre c. France*, 49620/15 ; *Deniau c. France*, 49621/15 ; *Ordre des avocats au barreau de Paris c. France*, 55058/15 ; *Sur c. France*, 55061/15 ; *Eydoux c. France*, 59602/15 ; *Conseil national des barreaux c. France*, 59621/15 ; *Syndicat national des journalistes et Fédération internationale des journalistes c. France,* 5763/16.