GRANDE CHAMBRE

AFFAIRE BIG BROTHER WATCH ET AUTRES
c. ROYAUME-UNI

(Requêtes n^os^ 58170/13, 62322/14 et 24969/15)

ARRÊT

Art 8 • Vie privée • Conformité à la Convention d'un régime de surveillance secrète, notamment de l'interception en masse de communications et du partage de renseignements • Nécessité de développer la jurisprudence au vu des différences importantes existant entre l'interception ciblée et l'interception en masse • Critère adapté à l'examen de régimes d'interception en masse au moyen d'une appréciation globale • Accent mis sur les « garanties de bout en bout » pour tenir compte de l'intensité croissante de l'atteinte au droit au respect de la vie privée au fur et à mesure que le processus d'interception en masse franchit les différentes étapes • Défaillances essentielles présentes dans le régime d'interception en masse à raison de l'absence d'autorisation indépendante, de l'absence de mention des catégories de sélecteurs dans les demandes de mandat et de l'absence d'autorisation interne préalable pour les sélecteurs liés à un individu identifiable • Prévisibilité et garanties suffisantes dans le régime de réception de renseignements provenant de services de renseignement étrangers • Régime d'acquisition de données de communication auprès de fournisseurs de services de communication non « prévu par la loi »

Art 10 • Liberté d'expression • Protection insuffisante d'éléments journalistiques confidentiels visés par des programmes de surveillance électronique

STRASBOURG

25 mai 2021

Cet arrêt est définitif. Il peut subir des retouches de forme.

En l'affaire Big Brother Watch et autres c. Royaume-Uni,

La Cour européenne des droits de l'homme, siégeant en une Grande Chambre composée de :

Robert Spano, *président,*
Jon Fridrik Kjølbro,
Angelika Nußberger,
Paul Lemmens,
Yonko Grozev,
Vincent A. De Gaetano,
Paulo Pinto de Albuquerque,
Faris Vehabović,
Iulia Antoanella Motoc,
Carlo Ranzoni,
Mārtiņš Mits,
Gabriele Kucsko-Stadlmayer,
Marko Bošnjak,
Tim Eicke,
Darian Pavli,
Erik Wennerström,
Saadet Yüksel, *juges,*

et de Søren Prebensen, *greffier adjoint de la Grande Chambre,*

Après en avoir délibéré en chambre du conseil le 11 juillet 2019, les 4 et 6 septembre 2019, et le 17 février 2021,

Rend l'arrêt que voici, adopté à cette dernière date :

PROCÉDURE

1. À l'origine de l'affaire se trouvent trois requêtes (n^{os} 58170/13, 62322/14 et 24969/15) dirigées contre le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et dont les personnes physiques ou morales énumérées en annexe (« les requérantes ») ont saisi la Cour le 4 septembre 2013, le 11 septembre 2014 et le 20 mai 2015 respectivement en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »).

2. Les requérantes ont été représentées respectivement par M^{e} D. Carey, du cabinet Deighton Pierce Glynn Solicitors, M^{e} R. Curling, du cabinet Leigh Day & Co. Solicitors, et M^{me} E. Norton, de l'association Liberty. Le gouvernement britannique (« le Gouvernement ») a été représenté par son ancien agent, M. C. Wickremasinghe, du ministère des Affaires étrangères et du Commonwealth.

3. Dans leurs requêtes, les requérantes se plaignaient de la portée et de l'ampleur des programmes de surveillance électronique mis en œuvre par le gouvernement britannique.

4. Les requêtes ont été communiquées au Gouvernement le 7 janvier 2014, le 5 janvier 2015 et le 24 novembre 2015 respectivement. Dans la première affaire, l'autorisation de se porter tiers intervenant a été accordée aux organismes suivants : Human Rights Watch, Access Now, Dutch Against Plasterk, Center For Democracy & Technology, le Réseau européen des institutions nationales des droits de l'homme, la Commission britannique pour l'égalité et les droits de l'homme (*Equality and Human Rights Commission*), la Fondation Helsinki pour les droits de l'homme, la Commission internationale de juristes, Open Society Justice Initiative, la Law Society of England and Wales et Project Moore. Dans la seconde affaire, l'autorisation de se porter tiers intervenant a été accordée aux organismes suivants : Center For Democracy and Technology, la Fondation Helsinki pour les droits de l'homme, la Commission internationale de juristes, le syndicat britannique des journalistes (*National Union of Journalists*) et la Media Lawyers' Association. Dans la troisième affaire, l'autorisation de se porter tiers intervenant a été accordée aux organismes suivants : Article 19, Electronic Privacy Information Center et la Commission britannique pour l'égalité et les droits de l'homme.

5. Le 4 juillet 2017, la chambre de la première section à laquelle l'affaire avait été attribuée a décidé de joindre les requêtes et de tenir une audience. Celle-ci s'est déroulée en public au Palais des droits de l'homme, à Strasbourg, le 7 novembre 2017. Le 13 septembre 2018, une chambre de ladite section, composée de Linos-Alexandre Sicilianos, Kristina Pardalos, Aleš Pejchal, Ksenija Turković, Armen Harutyunyan, Pauliine Koskelo et Tim Eicke, juges, ainsi que d'Abel Campos, greffier de section, a rendu un arrêt dans lequel elle déclarait irrecevables, à l'unanimité, les griefs formulés par les requérantes de la troisième affaire jointe sur le terrain des articles 6 et 10 – dans la mesure où elles invoquaient leur qualité d'ONG – et de l'article 14, et recevables leur autres griefs. Par ailleurs, elle déclarait recevables, à la majorité, les griefs formulés par les requérantes des première et deuxième affaires jointes. Elle concluait, à la majorité également, à la violation des articles 8 et 10 de la Convention à raison tant du régime découlant de l'article 8 § 4 de la RIPA que de celui instauré par le chapitre II de la RIPA, et à la non-violation de l'article 8 de la Convention en ce qui concerne le régime d'échange de renseignements. À cet arrêt se trouvaient joints l'exposé de l'opinion en partie concordante et en partie dissidente de la juge Koskelo, à laquelle la juge Turković s'est ralliée, ainsi que l'exposé de l'opinion partiellement dissidente et partiellement concordante commune aux juges Pardalos et Eicke.

6. Les 11 et 12 décembre 2018 respectivement, les requérantes des troisième et première affaires jointes ont sollicité le renvoi de l'affaire devant la Grande Chambre en vertu de l'article 43 de la Convention. Le 4 février 2019, le collège de la Grande Chambre a fait droit à leur demande.

7. La composition de la Grande Chambre a été arrêtée conformément aux articles 26 §§ 4 et 5 de la Convention et 24 du règlement de la Cour.

8. Tant les requérantes que le Gouvernement ont déposé des observations écrites sur la recevabilité et le fond de l'affaire (article 59 § 1 du règlement).

9. Le président de la Grande Chambre a autorisé les gouvernements français, néerlandais et norvégien, ainsi que le Rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, à intervenir dans la procédure écrite (articles 36 § 2 de la Convention et 44 § 3 du règlement).

10. Une audience s'est déroulée en public au Palais des droits de l'homme, à Strasbourg, le 10 juillet 2019.

Ont comparu :

a) *pour le Gouvernement*

MM. C. WICKREMASINGHE, *agent*,
J. EADIE Q.C. ET
J. MITFORD, *conseil*,
M. R. YARDLEY,
Mme L. MORGAN,
MM. H. MAWBY,
T. RUTHERFORD ET
J. KEAY-BRIGHT, *conseillers*;

b) *pour les requérantes*

M. B. JAFFEY Q.C.,
Mme H. MOUNTFIELD Q.C.,
MM. C. MCCARTHY,
R. MEHTA,
Mme G. SARATHY ET
M. D. HEATON, *conseils*,
M. D. CAREY ET
Mme R. CURLING, *conseillers*.

11. La Cour a entendu Mes Eadie, Jaffey et Mountfield en leurs déclarations et en leurs réponses aux questions qui leur ont été posées.

EN FAIT

I. LA GENÈSE DE L'AFFAIRE

12. Les trois requêtes ont été introduites à la suite des révélations faites par Edward Snowden sur les programmes de surveillance électronique mis en œuvre par les services de renseignement américains et britanniques.

13. Les requérantes, dont la liste figure en annexe, pensent toutes qu'en raison de la nature de leurs activités, leurs communications électroniques ont probablement été interceptées par les services de renseignement britanniques, obtenues par ces services auprès de gouvernements étrangers qui les avaient eux-mêmes interceptées, et/ou obtenues par les autorités britanniques auprès de fournisseurs de services de communication.

II. LES PROGRAMMES DE SURVEILLANCE SECRÈTE D'INTERNET EN CAUSE DANS LA PRÉSENTE AFFAIRE

14. Les communications Internet sont principalement acheminées par des réseaux internationaux de câbles sous-marins de fibre optique exploités par les fournisseurs de services de communication. Chaque câble peut regrouper plusieurs canaux de transmission (*bearers*), et Internet comprend environ 100 000 de ces canaux au niveau mondial. Chaque communication sur Internet est divisée en « paquets » de données, qui peuvent être transmis séparément les uns des autres sur différents canaux. Ces paquets sont acheminés de manière à emprunter la combinaison de chemins la plus rapide et la moins chère. Ainsi, une partie ou la totalité des paquets d'une communication adressée par une personne à une autre, que ce soit au Royaume-Uni ou à l'étranger, peut passer par un ou plusieurs autres pays en fonction du chemin optimal pour le fournisseur de services de communication concerné.

A. Le Royaume-Uni

1. L'interception en masse

15. Selon informations révélées par Edward Snowden en 2013, le service britannique du renseignement électronique (*Government Communications Headquarters* – « le GCHQ », l'un des services de renseignement britanniques) avait engagé une opération portant le nom de code « TEMPORA », qui lui permettait d'intercepter d'énormes volumes de données à partir des canaux de transmission et les conserver. Les autorités britanniques n'ont ni confirmé ni démenti l'existence d'une opération portant le nom de code TEMPORA.

16. Toutefois, selon un rapport rendu par la commission parlementaire sur le renseignement et la sécurité (*Intelligence and Security Committee*) en mars 2015 (« le rapport de la commission parlementaire », voir les paragraphes 142-149 ci-dessous), le GCHQ utilisait à l'époque pertinente deux grands systèmes de traitement des données pour l'interception en masse (*bulk interception*) de communications.

17. Le premier des deux systèmes de traitement des données mentionnés dans le rapport de la commission parlementaire ciblait une très faible proportion des canaux de transmission. Au fur et à mesure que les

communications transitaient par les canaux de transmission ciblés, le système comparait le trafic avec une liste de « sélecteurs simples » (*simple selectors*). Les sélecteurs simples étaient des identifieurs (*identifiers*) spécifiques (par exemple, une adresse de courrier électronique) liés à une cible connue. Toutes les communications correspondant à un sélecteur étaient collectées, les autres étaient automatiquement écartées. Les analystes procédaient ensuite à un « triage » des communications collectées pour déterminer lesquelles présentaient le plus d'intérêt pour le renseignement et devaient donc être ouvertes et lues. En pratique, seule une très faible proportion des éléments collectés par ce processus étaient ouverts et lus par les analystes. Selon le rapport de la commission parlementaire, le GCHQ ne disposait pas de ressources suffisantes pour lire toutes les communications.

18. Le second système de traitement des données visait un nombre encore plus réduit de canaux de transmission (un sous-ensemble de ceux concernés par le processus décrit au paragraphe précédent), qui étaient choisis comme étant les plus susceptibles de transmettre des communications présentant un intérêt pour le renseignement. Le traitement avait lieu en deux temps : d'abord, on appliquait un ensemble de « règles de traitement » qui visaient à écarter les éléments les moins susceptibles de présenter un intérêt ; les éléments issus de cette sélection faisaient ensuite l'objet d'un ensemble de requêtes complexes qui visaient à isoler ceux qui étaient susceptibles de présenter le plus d'intérêt pour le renseignement. Ces recherches généraient un index, et seuls les éléments figurant dans cet index étaient susceptibles d'être examinés par les analystes. Toutes les communications qui ne figuraient pas dans l'index devaient être supprimées.

19. Le cadre juridique qui régissait au moment des faits l'interception en masse de communications est décrit en détail ci-dessous, dans la section intitulée « Le droit interne pertinent ». En bref, l'article 8 § 4 de la loi de 2000 portant réglementation des pouvoirs d'enquête (*Regulation of Investigatory Powers Act 2000*, « la RIPA », paragraphe 72 ci-dessous) permettait au ministre compétent d'émettre des mandats d'« interception de communications extérieures », tandis que l'article 16 de cette loi (paragraphes 84-92 ci-dessous) interdisait de sélectionner pour lecture, consultation ou écoute les éléments interceptés « selon un facteur lié à un individu dont on sa[va]it qu'il se trouv[ait] [à ce moment-là] dans les îles Britanniques ».

2. L'échange de renseignements

20. Le chapitre 12 du code de conduite en matière d'interception de communications (paragraphe 116 ci-dessous) tel qu'en vigueur à l'époque pertinente définissait les conditions dans lesquelles les services de renseignement britanniques pouvaient demander des informations à des services de renseignement étrangers et les procédures à respecter pour soumettre de telles demandes. Ce chapitre avait été ajouté au code de

conduite en matière d'interception de communications après que le Tribunal des pouvoirs d'enquête (*Investigatory Powers Tribunal*, « l'IPT ») eut ordonné aux services de renseignement de révéler leurs procédures d'échange d'informations dans le cadre de la procédure engagée par les requérantes dans la troisième des affaires jointes (« l'affaire *Liberty* » – paragraphes 28-60 ci-dessous).

3. L'acquisition de données de communication auprès des fournisseurs de services de communication

21. Le chapitre II de la RIPA et le code de conduite sur l'acquisition de données de communication qui l'accompagnait régissaient la procédure par laquelle certaines autorités publiques pouvaient demander aux fournisseurs de services de communication de leur fournir des données de communication (paragraphes 117-121 ci-dessous).

B. Les États-Unis

22. L'Office national de sécurité américain (*National Security Agency*, « la NSA ») a reconnu l'existence de deux opérations, appelées respectivement PRISM et Upstream.

1. PRISM

23. PRISM est un programme dans le cadre duquel le gouvernement des États-Unis obtient des éléments présentant un intérêt pour le renseignement (par exemple des communications) auprès des fournisseurs de services Internet. L'accès aux données dans le cadre du programme PRISM est spécifique et ciblé (par opposition au forage de données (*data mining*), qui est beaucoup plus large). Les autorités américaines ont indiqué que ce programme relève de la loi sur la surveillance opérée aux fins du renseignement extérieur (*Foreign Intelligence Surveillance Act*, « la FISA »), et que les demandes d'accès à des données dans le cadre de PRISM doivent être approuvées par la Cour de surveillance du renseignement étranger (*Foreign Intelligence Surveillance Court* – « FISC »).

24. Il ressort des documents de la NSA divulgués par Edward Snowden que le GCHQ a accès à PRISM depuis juillet 2010 et qu'il l'a utilisé pour produire des rapports de renseignement. Le GCHQ a reconnu avoir obtenu des États-Unis des informations recueillies dans le cadre du programme PRISM.

2. Upstream

25. Il ressort également des documents divulgués par Edward Snowden que le programme Upstream permet de collecter des données de contenu et

des données de communication à partir des câbles de fibre optique et de l'infrastructure des fournisseurs de services de communication américains. Il ouvre ainsi un large accès aux données mondiales, notamment à celles de personnes qui ne sont pas américaines. Ces données peuvent être collectées et conservées, et faire l'objet de recherches par mots-clés (pour de plus amples informations, voir les paragraphes 261-264 ci-dessous).

III. LA PROCÉDURE INTERNE DANS LES PREMIÈRE ET LA DEUXIÈME DES AFFAIRES JOINTES (« LES DEUX PREMIÈRES AFFAIRES »)

26. Le 3 juillet 2013, les requérantes de la première des affaires jointes (requête n° 58170/13) adressèrent au Gouvernement une lettre de protocole préalable à l'instance (*pre-action protocol letter*) dans laquelle elles énonçaient leurs griefs et demandaient aux autorités de déclarer que les articles 1 et 3 de la loi de 1994 sur les services de renseignement (*Intelligence Services Act 1994* – « la loi sur les services de renseignement », paragraphes 108 et 110 ci-dessous), l'article 1 de la loi de 1989 sur les services de sécurité (*Security Services Act 1989*, « la loi sur les services de sécurité », paragraphe 106 ci-dessous) et l'article 8 de la RIPA (paragraphe 66 ci-dessous) étaient incompatibles avec la Convention. Le 26 juillet 2013, le gouvernement britannique répondit que l'article 65 § 2 de la RIPA avait pour effet d'exclure la compétence de la *High Court* quant aux griefs concernant le respect des droits de l'homme formulés contre les services de renseignement, mais que ces griefs pouvaient être portés devant l'IPT, tribunal spécialisé instauré par la RIPA pour examiner les allégations de citoyens s'estimant victimes, de la part des autorités, d'une ingérence illicite dans leurs communications à l'occasion des activités relevant de cette loi. Il précisait que ce tribunal était seul compétent pour examiner tout grief d'une personne pensant que ses communications avaient été interceptées et, si tel avait été le cas, pour examiner la base de cette interception (paragraphes 122-133 ci-dessous). Les requérantes n'entreprirent pas de démarches supplémentaires.

27. Les requérantes de la deuxième des affaires jointes (requête n° 62322/14) n'ont engagé aucune procédure au niveau interne car elles estimaient ne pas disposer d'un recours effectif relativement à leurs griefs fondés sur la Convention.

IV. LA PROCÉDURE INTERNE DANS LA TROISIÈME DES AFFAIRES JOINTES (« LA TROISIÈME AFFAIRE »)

28. Les dix organisations de défense des droits de l'homme requérantes dans la troisième des affaires jointes (requête n° 24960/15) ont chacune porté leurs griefs devant l'IPT entre juin et décembre 2013 (« l'affaire

Liberty »). Elles alléguaient que les services de renseignement, le ministre de l'Intérieur et le ministre des Affaires étrangères avaient violé les articles 8, 10, et 14 de la Convention, i) en accédant à des communications interceptées par le gouvernement américain dans le cadre des programmes PRISM et Upstream et aux données de communication associées ou en les obtenant d'une autre façon (« le grief PRISM »), et ii) en interceptant, en inspectant et en conservant leurs communications et les données de communication associées dans le cadre du programme TEMPORA (« le grief tiré de l'article 8 § 4 de la RIPA »).

29. Le 14 février 2014, l'IPT ordonna la jonction des dix affaires. Il désigna ensuite un Conseil près le Tribunal (*Counsel to the Tribunal*, paragraphe 132 ci-dessous). Le Conseil près le Tribunal est chargé d'assister l'IPT selon les demandes de celui-ci, notamment en faisant des déclarations sur les points à l'égard desquels les parties ne peuvent pas toutes être représentées (par exemple pour des raisons tenant à la sécurité nationale).

30. Dans sa réponse aux allégations des requérantes, le Gouvernement adopta une ligne « ni-ni », c'est-à-dire qu'il ne confirma ni n'infirma les allégations selon lesquelles les communications des intéressées avaient été interceptées. Il fut donc convenu que l'IPT statuerait sur les points de droit en se fondant sur la présomption que, d'une part, la NSA avait obtenu les communications et les données de communication des requérantes dans le cadre du programme PRISM ou du programme Upstream et les avait transmises au GCHQ, qui les avait conservées, stockées, analysées et partagées, et, d'autre part, que le GCHQ avait intercepté les communications et les données de communication des requérantes dans le cadre du programme TEMPORA et les avait conservées, stockées, analysées et partagées. La question était de savoir si, sur la base de ces faits présumés, l'interception, la conservation, le stockage et le partage de ces données étaient compatibles avec les articles 8 et 10 de la Convention, pris isolément et combinés avec l'article 14.

A. L'audience

31. L'IPT, composé de deux juges de la *High Court*, d'un *circuit judge* et de deux avocats chevronnés (*senior barristers*), tint audience publiquement pendant cinq jours, du 14 au 18 juillet 2014. Le Gouvernement lui demanda de tenir une audience supplémentaire à huis clos afin d'examiner les procédures internes non publiques de traitement des éléments interceptés appliquées par le GCHQ, qui avaient été qualifiées pendant l'audience publique d'« œuvres vives » (ci-après « les procédures non publiques »). Les requérantes s'y opposèrent, arguant qu'il ne se justifiait pas de tenir une audience à huis clos et qu'il était inéquitable de ne pas leur révéler les procédures en question.

32. L'IPT fit droit à la demande de tenue d'une audience à huis clos en vertu de l'article 9 de son règlement (paragraphe 129 ci-dessous). Le 10 septembre 2014, une audience à huis clos fut tenue par l'IPT, qui bénéficiait « de l'assistance apportée par la participation pleine, éclairée et neutre (...) du conseil près le Tribunal », lequel avait pour rôle : i) de déterminer les documents, les passages des documents ou les éléments essentiels à divulguer ; ii) de faire valoir les arguments militant en faveur de la divulgation dans l'intérêt des plaignantes et de la transparence de la justice ; et iii) de veiller à ce que tous les arguments de droit et de fait pertinents (du point de vue des plaignantes) soient soulevés devant l'IPT.

33. Pendant l'audience à huis clos, l'IPT examina les procédures internes non publiques encadrant la conduite et la pratique des services de renseignement. Le 9 octobre 2014, il avisa les requérantes qu'il estimait que certains des éléments examinés à huis clos pouvaient être divulgués. Il précisait qu'il avait invité le Gouvernement à divulguer ces éléments et que celui-ci y avait consenti. Lesdits éléments furent donc communiqués aux requérantes par une note (« la note de divulgation du 9 octobre »), et les parties furent invitées à adresser à l'IPT leurs observations sur les éléments en question.

34. Les requérantes demandèrent des informations sur le contexte et la source des éléments divulgués mais l'IPT refusa de leur donner plus de détails. Elles communiquèrent leurs observations écrites sur ces éléments.

35. Par la suite, les défendeurs modifièrent et complétèrent les éléments divulgués.

36. À l'issue des dernières modifications, faites le 12 novembre 2014, la note de divulgation datée du 9 octobre indiquait ceci :

> « Le gouvernement américain a reconnu publiquement que le système PRISM et le programme Upstream (...) permettent d'acquérir, dans le but de recueillir des informations présentant un intérêt pour le renseignement extérieur, des communications adressées à des sélecteurs spécifiques ciblés liés à des personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis, des communications provenant de ces sélecteurs ou des communications en rapport avec ces sélecteurs. Dans la mesure où le gouvernement américain permet aux services de renseignement de demander la communication d'éléments obtenus dans le cadre du système PRISM (et/ou (...) du programme Upstream), ces demandes ne peuvent concerner que des communications interceptées non analysées (ainsi que les données de communication associées) acquises de cette manière.
>
> 1. Hors du cadre d'un accord d'entraide judiciaire internationale, les services de renseignement ne peuvent demander au gouvernement d'un pays ou territoire non britannique des communications interceptées non analysées (ainsi que les données de communication associées) que :
>
> a. lorsqu'un mandat d'interception pertinent a déjà été émis en vertu de [la RIPA] par le ministre, que l'assistance d'un gouvernement étranger est nécessaire pour obtenir les communications en question parce qu'il n'est pas possible de les obtenir dans le cadre de ce mandat d'interception, et que leur acquisition par les services de renseignement est nécessaire et proportionnée au but visé ; ou

b. lorsqu'en l'absence de mandat d'interception pertinent émis en vertu de la RIPA, le fait de demander ces communications ne constitue pas un contournement délibéré de la RIPA et n'est pas contraire au principe établi dans *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997 [selon lequel les organes publics doivent exercer leurs pouvoirs discrétionnaires pour promouvoir l'esprit et l'objet de la loi qui les a investis de ces pouvoirs (et non pour les contourner)] (par exemple, les communications sont demandées parce qu'il n'est pas faisable techniquement de les obtenir au moyen d'une interception réalisée en vertu de la RIPA), et que leur acquisition par les services de renseignement est nécessaire et proportionné au but visé. En pareil cas, la question de savoir si la demande doit être faite est examinée et tranchée par le ministre en personne. Ce type de demande ne peut intervenir que dans des circonstances exceptionnelles, et aucune demande de ce type n'avait été faite à la date de la présente note.

(...)

2. Lorsque les services de renseignement reçoivent du gouvernement d'un pays ou territoire non britannique le contenu de communications interceptées ou des données de communication, qu'ils en aient ou non fait la demande, que le contenu ait ou non été analysé, et que les données de communication soient ou non associées au contenu des communications, le contenu des communications et les données de communication sont, en vertu des « procédures » internes, soumis aux mêmes règles et garanties internes que les contenus et données de même catégorie qui ont été obtenus directement par les services de renseignement au moyen d'une interception réalisée en vertu de la RIPA.

3. Les services de renseignement qui reçoivent des éléments interceptés non analysés et les données de communication associées à l'issue d'une interception réalisée sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA appliquent des « procédures » internes qui leur imposent d'inscrire dans un registre les raisons pour lesquelles l'accès à ces éléments interceptés non analysés est nécessaire, avant qu'une personne autorisée ne puisse y accéder en vertu de l'article 16 de la RIPA.

4. Les « procédures » internes appliquées par les services de renseignement qui reçoivent des éléments interceptés non analysés et les données de communication associées à l'issue d'une interception réalisée sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA fixent (ou imposent que soit déterminée système par système) une durée maximale de conservation pour les différentes catégories de données, en fonction de la nature des données en question et du degré de l'intrusion dans la vie privée résultant de leur collecte. Les durées ainsi fixées (ou déterminées) ne dépassent pas deux ans en principe, et dans certains cas elles sont bien plus courtes (étant entendu que les rapports de renseignement établis sur la base de ces données constituent une catégorie distincte et sont conservés plus longtemps). Les données ne peuvent être conservées au-delà de la durée maximale de conservation qui leur est applicable que sur autorisation préalable délivrée par un haut responsable du service de renseignement concerné au motif que la prolongation de leur conservation a été jugée nécessaire et proportionnée au but visé (si par la suite on estime que la prolongation de la conservation des données ne répond plus aux critères de nécessité et de proportionnalité, celles-ci sont supprimées). Dans la mesure du possible, le respect des durées de conservation des données est assuré par un processus de suppression automatisée qui se déclenche lorsque la durée maximale de conservation applicable aux données en question est atteinte. Les durées maximales de conservation des données font l'objet d'une supervision du Commissaire à l'interception des communications et sont fixées en accord avec lui. En ce qui concerne en particulier

les données de communication associées, Sir Anthony May a adressé une recommandation aux services de renseignement qui reçoivent des éléments interceptés non analysés et les données de communication associées à l'issue d'une interception réalisée sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA, et le Commissaire par intérim (Sir Paul Kennedy) s'est récemment déclaré satisfait de la mise en œuvre de cette recommandation.

5. Les « procédures » internes appliquées par les services de renseignement en vertu de [la loi de 1989 sur les services de sécurité], de [la loi de 1994 sur les services de renseignement] et des articles 15 et 16 de la RIPA sont réexaminées régulièrement afin qu'elles restent à jour et effectives. De plus, dans le cadre de ces révisions, il est désormais loisible aux services de renseignement d'apprécier s'il serait sûr et utile de rendre publiques davantage de procédures internes (par exemple, en les insérant dans un code de conduite officiel). »

B. Le premier jugement de l'IPT (5 décembre 2014)

37. Le 5 décembre 2014, l'IPT rendit son premier jugement. Celui-ci portait sur les procédures alors applicables en matière d'interception de communications et de réception de communications interceptées par les services de renseignements étrangers.

1. Le grief PRISM

38. L'IPT admit que le grief PRISM faisait entrer en jeu l'article 8 de la Convention, mais à un degré « moindre » que le grief examiné par la Cour dans l'affaire *Weber et Saravia c. Allemagne* (déc.) (n° 54934/00, CEDH 2006‑XI). Il considéra donc qu'il fallait que les autorités qui prenaient part au traitement de communications obtenues auprès de services de renseignement étrangers respectent les exigences découlant de l'article 8, notamment quant au stockage, au partage, à la conservation et à la destruction de ces communications. S'appuyant sur les arrêts *Bykov c. Russie* [GC] (n° 4378/02, §§ 76 et 78, 10 mars 2009) et *Malone c. Royaume-Uni* (2 août 1984, série A n° 82), l'IPT estima que pour que l'on puisse considérer que l'ingérence était « prévue par la loi », le pouvoir d'appréciation accordé à l'exécutif ne devait pas être illimité, et que la nature des règles devait au contraire être claire et leur champ d'application divulgué au public, dans la mesure du possible. Toutefois, renvoyant à l'arrêt *Leander c. Suède* (26 mars 1987, § 51, série A n° 116), il jugea évident que dans le domaine de la sécurité nationale, l'obligation de publicité était beaucoup plus restreinte et le degré de prévisibilité requis par l'article 8 devait être réduit, faute de quoi le but même des mesures prises pour protéger la sécurité nationale serait mis en péril.

39. L'IPT tint le raisonnement suivant :

« 41. Nous considérons qu'il faut qu'il y ait une information suffisante quant aux règles ou procédures qui ne sont pas divulguées (...) Nous sommes convaincus que dans le domaine de l'échange de renseignements, on ne peut s'attendre à ce que les

règles doivent figurer dans une loi (*Weber*) ni même dans un code (comme l'exigeait la Cour [européenne] dans l'arrêt qu'elle a rendu en l'affaire *Liberty [c. Royaume-Uni*, nº 58243/00, 1er juillet 2008]). Nous estimons suffisant :

i) qu'il existe des règles ou procédures appropriées dont l'existence soit connue du public et reconnue, et que leur teneur soit suffisamment dévoilée pour que l'on sache en quoi elles consistent (voir l'arrêt *Malone* (...)), et

ii) que ces règles ou procédures fassent l'objet d'un contrôle approprié. »

40. L'IPT nota que les procédures relatives au partage d'informations étaient prévues par le cadre légal instauré par la loi de 1989 sur les services de sécurité (paragraphes 105-106 ci-dessous) et la loi de 1994 sur les services de renseignement (paragraphes 107-110 ci-dessous). Il tint compte également d'une déposition faite dans l'affaire *Liberty* par le directeur général de l'Office pour la sécurité et la lutte contre le terrorisme (*Office for Security and Counter Terrorism (OSCT)*) du ministère de l'Intérieur, Charles Farr, qui expliquait que le cadre légal posé par ces lois était sous-tendu par des directives internes détaillées, notamment des procédures visant à assurer que les services concernés ne puissant obtenir que les informations nécessaires au bon exercice de leurs fonctions. M. Farr ajoutait que les agents suivaient une formation obligatoire sur le cadre juridique et politique dans lequel ils agissaient, et qu'ils recevaient des instructions claires quant à la nécessité de respecter scrupuleusement la loi et les directives internes. Enfin, il expliquait que les détails complets des procédures appliquées étaient confidentiels car il n'aurait pas été possible de les publier sans risque d'atteinte aux intérêts de la sécurité nationale.

41. L'IPT reconnut que faute d'être portées à la connaissance du public, même sous une forme sommaire, les procédures en question n'étaient pas accessibles. Il accorda cependant du poids au fait qu'elles étaient soumises aux pouvoirs de contrôle et d'enquête de la commission parlementaire sur le renseignement et la sécurité et du Commissaire à l'interception des communications. En outre, il considéra qu'il était lui-même en mesure d'exercer un contrôle puisqu'il avait accès à toutes les informations secrètes et qu'il pouvait suspendre l'audience publique pour tenir une audience à huis clos afin de s'assurer de l'existence des procédures mentionnées par M. Farr et de leur aptitude à assurer la protection de l'individu contre les ingérences arbitraires.

42. Après avoir examiné les procédures non publiques, l'IPT conclut que la note de divulgation du 9 octobre (telle que modifiée ultérieurement, paragraphes 33 et 36 ci-dessus) résumait de manière claire et exacte cette partie des éléments examinés à huis clos, et que les autres éléments présentés lors de l'audience à huis clos étaient trop sensibles pour être divulgués sans risque d'atteinte à la sécurité nationale et au principe consistant à ne confirmer ni démentir les hypothèses avancées. Il se déclara également convaincu que les conditions préalables à une demande d'informations au gouvernement des États-Unis d'Amérique étaient claires

en ce qu'elles exigeaient l'existence d'un mandat émis en vertu de l'article 8 § 1 de la RIPA ou d'un mandat émis en vertu de l'article 8 § 4 dont relevaient les communications de la cible envisagée et, si l'on savait que l'individu se trouvait dans les îles Britanniques, d'un document modificatif approprié établi conformément à l'article 16 § 3) (paragraphe 86 ci-dessous). Il estima en conséquence que toute demande relative à des communications interceptées ou à des données de communication provenant des programmes PRISM ou Upstream serait soumise au régime découlant de la RIPA, à moins qu'elle ne relève du cas tout à fait exceptionnel décrit au point 1 b) de la note de divulgation telle que modifiée – cas qui ne s'était jamais présenté.

43. L'IPT releva néanmoins le « sujet de préoccupation » suivant :

> « Il est vrai que toute demande ou réception de communications interceptées ou de données de communication provenant des programmes PRISM et/ou Upstream est normalement soumise aux mêmes garanties que l'obtention de communications ou de données de communication directement par les défendeurs. Cependant, s'il était fait une demande relevant du point 1 b), il serait possible – bien qu'en pareil cas la demande doive recevoir l'aval du ministre et les éléments obtenus doivent être traités dans le respect des dispositions de la RIPA – que la protection apportée par l'article 16 ne s'applique pas. Comme indiqué précédemment, il n'a jamais été fait en pratique de demande relevant du point 1 b), et il n'y a donc pas eu de problème jusqu'à présent. Nous considérons toutefois que devrait être instaurée une procédure qui prévoirait que toute demande de ce type qui viendrait à être faite devrait, au moment de sa transmission au ministre, traiter la question de l'article 16 § 3. »

44. Toutefois, sous cette réserve, il parvint aux conclusions suivantes :

> « i) Après avoir examiné les procédures non publiques, comme exposé dans le présent jugement, nous estimons que des procédures permettant d'assurer de manière satisfaisante le respect du cadre légal et des articles 8 et 10 de la Convention ont été mises en place en ce qui concerne la réception de données provenant d'interceptions réalisées dans le cadre des programmes PRISM et/ou Upstream.
>
> ii) Bien entendu, cela n'est pas suffisant en soi, car ces procédures doivent également être suffisamment accessibles au public. Nous considérons que le cadre juridique susmentionné et les déclarations de la commission parlementaire et du Commissaire dont nous avons fait état assurent une publicité suffisante aux procédures en question, et qu'à présent, à l'issue des deux audiences que nous avons tenues à huis clos, elles ont été suffisamment divulguées au public par les défendeurs et exposées dans le présent jugement.
>
> iii) Ces procédures sont soumises à un contrôle.
>
> iv) Il s'ensuit que, conformément à l'arrêt *Bykov* (voir le paragraphe 37 ci-dessus), l'étendue du pouvoir discrétionnaire des défendeurs en matière de réception et de traitement des éléments interceptés et des données de communication, et – sous réserve des points relatifs à l'article 8 § 4 de la RIPA indiqués ci-dessous – les modalités d'exercice de ce pouvoir, sont accessibles [et définies] de manière suffisamment claire pour fournir à l'individu une protection adéquate contre l'arbitraire. »

45. Enfin, l'IPT répondit à un argument avancé seulement par Amnesty International, qui consistait à dire que l'article 8 de la Convention mettait à la charge du Royaume-Uni l'obligation positive de prévenir ou de contrecarrer les interceptions de communications par les États-Unis, et que cette obligation lui interdisait notamment de donner son aval à ces interceptions en acceptant de s'en voir communiquer les résultats. Citant l'arrêt *M. et autres c. Italie et Bulgarie* (n° 40020/03, § 127, 31 juillet 2012), l'IPT releva que « les organes de la Convention [avaient] dit à plusieurs reprises que celle-ci ne garant[issait] pas le droit d'obliger une Haute Partie contractante à exercer une protection diplomatique, ou à épouser la cause d'un requérant sur le plan du droit international ou à intervenir en son nom auprès des autorités d'un État tiers ». En conséquence, il rejeta l'argument d'Amnesty International.

2. Le grief tiré de l'article 8 § 4 de la RIPA

46. L'IPT estima que pour statuer sur la compatibilité avec la Convention du régime découlant de l'article 8 § 4 de la RIPA (qui établissait le cadre juridique de l'interception en masse de communications extérieures), il fallait répondre aux quatre questions suivantes :

> « 1) La distinction entre les communications extérieures et les communications intérieures est-elle (...) difficile à opérer au point de priver de base légale le régime découlant de l'article 8 § 4 de la RIPA, en violation de l'article 8 § 2 de la Convention ?
>
> 2) Pour autant que l'article 16 de la RIPA pose une garantie nécessaire pour que l'ingérence dans les droits garantis par l'article 8 de la Convention soit prévue par la loi, cette garantie est-elle suffisante ?
>
> 3) Le régime ici en cause répond-il suffisamment, avec ou sans l'article 16, aux critères énoncés dans la décision *Weber*, pour autant qu'il doive y satisfaire pour être prévu par la loi ?
>
> 4) L'article 16 § 2 constitue-t-il une discrimination indirecte au sens de l'article 14 de la Convention, et, dans l'affirmative, peut-il se justifier ? »

47. Sur la première question, les requérantes arguaient que du fait des « bouleversements qu'[avait] connus la technologie depuis l'an 2000 », le nombre de communications extérieures avait considérablement augmenté, et qu'en conséquence, la distinction entre communications intérieures et communications extérieures posée à l'article 8 § 4 de la RIPA n'était plus « adaptée ». L'IPT admit que la technologie avait fortement évolué, et qu'il était impossible de différencier au stade de l'interception les communications extérieures des communications intérieures, mais il estima que les différences de vues quant à la définition précise de l'expression « communications extérieures » ne rendaient pas en elles-mêmes le régime découlant de l'article 8 § 4 de la RIPA incompatible avec l'article 8 § 2 de la Convention. À cet égard, il considéra que la difficulté qu'il y avait à

distinguer les communications « intérieures » des communications « extérieures » existait depuis l'adoption de la RIPA et que l'évolution de la technologie n'avait pas substantiellement accru la quantité ni la proportion des communications dont on ne pouvait savoir si elles étaient extérieures ou intérieures au moment de l'interception. Au pire, estimait-il, cette évolution avait « accéléré le processus qui [faisait] que plus de choses en ce monde, à bien y réfléchir, [dépassaient] le cadre des frontières nationales ». En toute hypothèse, poursuivait-il, cette distinction n'était pertinente qu'au stade de l'interception : le « gros du travail » était fait par l'application de l'article 16 de la RIPA, qui interdisait que les éléments interceptés soient sélectionnés pour être lus, consultés ou écoutés « selon un facteur lié à un individu dont on [savait] qu'il se [trouvait] dans les îles Britanniques » (paragraphes 84-92 ci-dessous). Il ajouta que l'on ne pouvait envisager d'examiner une communication interceptée sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA que dans les conditions prévues à l'article 16.

48. Sur la seconde question, l'IPT jugea suffisantes les garanties offertes par l'article 16, qui ne s'appliquaient qu'aux éléments interceptés et non aux données de communication associées. Il considéra que les données de communication relevaient aussi des critères *Weber* mais que l'article 15 (paragraphes 77-82 ci-dessous) offrait une protection et des garanties suffisantes à cet égard, et il estima que le fait que l'article 16 protégeait davantage le contenu des communications que les données associées constituait une différence justifiée et proportionnée car il était nécessaire de disposer des données de communication pour identifier les individus dont les communications interceptées étaient couvertes par l'article 16 (c'est-à-dire ceux dont on savait qu'ils se trouvaient dans les îles Britanniques).

49. Sur la troisième question, l'IPT conclut que le régime découlant de l'article 8 § 4 de la RIPA répondait suffisamment aux critères *Weber* (c'est-à-dire aux critères énoncés dans la décision *Weber et Saravia*, précitée, § 95 ; voir aussi les paragraphes 274 et 335 ci-dessous) et qu'en toute hypothèse, les mesures relevant de ce régime étaient « prévues par la loi ». S'agissant des deux premières exigences, il considéra que le renvoi à la « sécurité nationale » était suffisamment clair (au regard de la décision *Esbester c. Royaume-Uni* (déc.) (n° 18601/91, 2 avril 1993) et de l'arrêt *Kennedy c. Royaume-Uni* (n° 26839/05, 18 mai 2010)); que l'absence de ciblage au stade de l'interception était acceptable et inévitable, de même que dans l'affaire *Weber* ; qu'à première vue, les dispositions du paragraphe 5.2 du code de conduite en matière d'interception de communications, combiné avec les paragraphes 2.4, 2.5, 5.3, 5.4, 5.5 et 5.6 (paragraphe 96 ci-dessous), étaient satisfaisantes ; qu'il n'y avait pas lieu d'inclure des mots-clés de recherche dans les demandes de mandat ni dans les mandat eux-mêmes, car pareille exigence aurait inutilement compromis et limité la mise en œuvre

des mandats tout en risquant de s'avérer illusoire; et qu'il n'était pas impératif que le mandat soit soumis à une autorisation judiciaire.

50. Pour déterminer s'il était satisfait aux troisième, quatrième, cinquième et sixième critères *Weber*, l'IPT tint compte des garanties offertes par les articles 15 et 16 de la RIPA, du code de conduite en matière d'interception de communications et des procédures « non publiques ». Il estima inutile que les détails précis de toutes les garanties soient publiés ou énoncés dans la loi ou le code de conduite. Il considéra à cet égard qu'il était possible, particulièrement dans le domaine de la sécurité nationale, de tenir compte de procédures administratives confidentielles, procédures que par définition l'exécutif pouvait modifier sans en référer au Parlement, pour autant que les informations divulguées indiquent l'étendue du pouvoir discrétionnaire des autorités et la manière dont elles l'exerçaient. Il précisa que cela était particulièrement vrai lorsque, comme c'était le cas en l'occurrence, le code de conduite renvoyait aux procédures en question et qu'un régime de supervision (exercé par le Commissaire, par l'IPT lui-même et par la commission parlementaire) garantissait que ces procédures faisaient l'objet d'un contrôle. Il se déclara convaincu, compte tenu de ce qu'il avait entendu lors de l'audience à huis clos, que les autorités n'étaient pas en train de constituer une grande base de données de communication, et que des procédures adéquates régissaient la durée de conservation des données et leur destruction. Il estima, comme il l'avait fait pour le grief PRISM, que la loi, le code de conduite, les rapports du Commissaire et, désormais, son propre jugement assuraient une publicité suffisante aux procédures prévues par l'article 8 § 4 de la RIPA.

51. Sur la quatrième et dernière question, l'IPT ne trancha pas le point de savoir si l'application de régimes différents selon que les individus concernés se trouvaient ou non dans les îles Britanniques était constitutive d'une discrimination indirecte à raison de l'origine nationale, estimant que même si tel avait été le cas, la différence de traitement aurait été suffisamment justifiée par le fait qu'il était plus difficile d'enquêter sur des projets terroristes ou criminels ourdis à l'étranger. Il observa également que l'accès aux communications extérieures visait principalement à l'obtention d'informations sur les personnes se trouvant à l'étranger et que si l'on avait éliminé la distinction examinée, il aurait fallu dans presque tous les cas obtenir un certificat en vertu de l'article 16 § 3 de la RIPA (qui autorisait, dans des cas exceptionnels, l'accès aux données interceptées dans le cadre d'un mandat émis en vertu de l'article 8 § 4 relatives à des personnes se trouvant dans les îles Britanniques, voir le paragraphe 86 ci-dessous), ce qui aurait fortement compromis l'efficacité du régime découlant de l'article 8 § 4.

52. Enfin, les requérantes arguaient que la protection offerte par l'article 10 de la Convention devait s'appliquer aux organisations non gouvernementales (« ONG ») réalisant des enquêtes de la même manière

qu'elle s'appliquait aux journalistes. Amnesty International avait d'abord allégué devant l'IPT qu'il n'existait probablement pas de procédure adéquate en ce qui concernait les éléments couverts par le secret professionnel des avocats. Ce grief fut par la suite « transféré » de l'affaire dont il est ici question à l'affaire *Belhadj* (paragraphes 99-101 ci-dessous), dans laquelle Amnesty International se joignit aux autres demandeurs. Aucun moyen analogue tiré de la confidentialité des données recueillies par les ONG n'avait été avancé avant le 17 novembre 2014 (après la première et la seconde audiences publiques). Estimant que ce moyen aurait pu être soulevé à n'importe quel moment, l'IPT conclut dans son jugement qu'il l'avait été « bien trop tard » pour être examiné dans le cadre de la procédure.

53. Quant aux autres griefs formulés sur le terrain de l'article 10 de la Convention, l'IPT estima qu'ils ne renfermaient aucun argument distinct ou supplémentaire par rapport à ce qui avait déjà été avancé sur le terrain de l'article 8. Bien qu'il eût évoqué l'arrêt *Sanoma Uitgevers B.V. c. Pays-Bas* [GC] (n° 38224/03, 14 septembre 2010), l'IPT releva que l'affaire des requérantes ne concernait pas la surveillance ciblée de journalistes ou d'ONG. Il considéra qu'en tout état de cause, dans le cadre d'une surveillance non ciblée opérée sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA, il était « clairement impossible » de prévoir qu'il faudrait demander, avant la délivrance du mandat, une autorisation judiciaire circonscrite aux éléments qui pourraient se révéler avoir une incidence sur les droits protégés par l'article 10. Il admit qu'il pourrait y avoir un problème dans l'hypothèse où, dans le cadre de l'examen de la teneur des communications, une question de confidentialité journalistique se poserait, mais il nota que le code de conduite en matière d'interception de communications renfermait des garanties supplémentaires encadrant le traitement de ce type de données.

54. Après la publication de son jugement, l'IPT invita les parties à lui présenter leurs observations sur deux points, les invitant à répondre, d'une part, à la question de savoir si le régime juridique critiqué dans le grief PRISM, tel qu'il était en vigueur avant les débats qui s'étaient tenus devant lui, était conforme aux articles 8 et 10 et, d'autre part, à exprimer leur avis sur la légalité et la proportionnalité de l'interception, à supposer qu'elle ait eu lieu, des communications des plaignantes. Il estima inutile que soient présentées des observations supplémentaires sur la proportionnalité du régime découlant de l'article 8 § 4 de la RIPA dans son ensemble.

C. Le deuxième jugement de l'IPT (6 février 2015)

55. Dans son deuxième jugement, rendu le 6 février 2015, l'IPT examina le point de savoir si les procédures concernant PRISM et Upstream en

vigueur avant son jugement de décembre 2014 étaient contraires à l'article 8 et/ou à l'article 10 de la Convention.

56. Il admit que seule la note de divulgation du 9 octobre telle que modifiée (paragraphes 33 et 36 ci-dessus) l'avait conduit à conclure que le régime alors en vigueur était « prévu par la loi ». Il estima qu'en l'absence de cette divulgation, il n'y aurait pas eu d'information suffisante au regard des articles 8 et 10 de la Convention. Il jugea donc qu'avant cette divulgation :

> « 23. (...) le régime de demande, de réception, de stockage et de transmission par les autorités britanniques de communications privées d'individus se trouvant au Royaume-Uni obtenues par les autorités américaines dans le cadre du programme PRISM et/ou (...) du programme Upstream était contraire aux articles 8 et 10 de la [Convention]. Il y est à présent conforme. »

D. Le troisième jugement de l'IPT (22 juin 2015, modifié par une lettre du 1er juillet 2015)

57. Dans son troisième jugement, rendu public le 22 juin 2015, l'IPT se prononçait sur les points de savoir, d'une part, si les autorités britanniques avaient enfreint les articles 8 et/ou 10 de la Convention en sollicitant, en recevant, en stockant ou transmettant les communications des requérantes obtenues dans le cadre des programmes PRISM ou Upstream et, d'autre part, si elles avaient intercepté, consulté, stocké ou transmis de manière illicite ou contraire aux articles 8 et/ou 10 de la Convention les communications des requérantes.

58. L'IPT rejeta les plaintes de huit des dix requérantes. Conformément à sa pratique habituelle en pareil cas, il ne confirma ni n'infirma l'hypothèse de l'interception de leurs communications. En revanche, il prononça une décision en faveur de deux requérantes. Le jugement du 22 juin comportait une erreur dans le nom de l'une de ces organisations, erreur qui fut corrigée par une lettre de l'IPT en date du 1er juillet 2015.

59. L'IPT conclut que des communications par courrier électronique d'Amnesty International avaient fait l'objet d'une interception et d'un accès licites et proportionnés au but visé, sur la base de l'article 8 § 4 de la RIPA, mais que les règles internes du GCHQ relatives à la durée maximale de conservation avaient été méconnues et que les données interceptées avaient en conséquence été conservées au-delà de la durée autorisée. Il estima toutefois établi que l'on n'avait pas accédé aux données en question après l'expiration de la date limite de conservation et que le non-respect des règles était donc purement technique. Jugeant néanmoins que ce manquement emportait violation de l'article 8 de la Convention, l'IPT ordonna au GCHQ de détruire toutes les communications qui avaient été conservées au-delà de la durée autorisée et d'en remettre une copie imprimée dans un délai de sept jours au Commissaire à l'interception des communications pour que celui-ci la conserve pendant cinq ans au cas où ces communications s'avéreraient

nécessaires pour une procédure en justice ultérieure. Il ordonna de plus au GCHQ de lui remettre dans un délai de quatorze jours un rapport confidentiel confirmant la destruction des données. Il n'octroya à Amnesty International aucune réparation.

60. L'IPT conclut également que des communications provenant d'une adresse de courrier électronique associée à Legal Resources Centre avaient été interceptées et sélectionnées pour examen dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA. Il considéra que l'interception avait été licite et proportionnée au but visé et que la sélection pour examen avait été proportionnée au but visé, mais il constata que, par erreur, on n'avait pas suivi la procédure interne de sélection. En conséquence, il conclut à la violation des droits de Legal Resources Centre tels que garantis par l'article 8 de la Convention. Il jugea toutefois établi que les données correspondantes n'avaient pas été utilisées et que rien n'avait été conservé, de sorte que Legal Resources Centre n'avait subi concrètement aucun inconvénient, dommage ou préjudice. Il considéra donc que son constat de violation valait satisfaction équitable et n'octroya à Legal Resources Centre aucune réparation.

LE CADRE ET LA PRATIQUE JURIDIQUES PERTINENTS

I. LE DROIT INTERNE PERTINENT

A. L'interception de communications

1. Les mandats : dispositions générales

61. L'article 1 § 1 de la RIPA de 2000, dont les dispositions ont été abrogées et remplacées par celles de la loi de 2016 sur les pouvoirs d'enquête (*Investigatory Powers Act 2016*), interdisait l'interception de toute communication au cours de sa transmission par un service postal public ou un système de télécommunication public, sauf en vertu d'un mandat délivré sur le fondement de l'article 5 (« mandat d'interception »).

62. L'article 5 § 2 permettait au ministre compétent de délivrer un mandat d'interception s'il estimait, premièrement, que cette mesure était nécessaire pour les motifs énoncés à l'article 5 § 3, à savoir la protection de la sécurité nationale, la prévention ou la détection des infractions graves, ou la sauvegarde de la prospérité économique du Royaume-Uni (dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale, voir les paragraphes 3.5 et 6.11 du code de conduite en matière d'interception de communication reproduits au paragraphe 96 ci-dessous) et, deuxièmement, que l'opération autorisée par le mandat était proportionnée au but visé par celle-ci. Pour apprécier la nécessité et la proportionnalité de pareille mesure, il fallait tenir compte du point de savoir si les informations dont le mandat

visait à permettre l'obtention auraient raisonnablement pu être recueillies par d'autres moyens.

63. Selon l'article 81 § 2 b) de la RIPA, les « infractions graves » étaient celles qui répondaient à l'un des critères suivants :

> « a) l'infraction ou l'une des infractions qui est ou serait constituée par la conduite est une infraction pour laquelle une personne âgée de vingt et un ans révolus et n'ayant jamais été condamnée pourrait raisonnablement s'attendre à être condamnée à une peine de prison de trois ans ou plus ;
>
> b) la conduite comprend l'usage de la violence, aboutit à un gain financier important ou est le fait d'un grand nombre de personnes agissant dans un but commun. »

64. L'article 81 § 5 était ainsi libellé :

> « Aux fins de la présente loi, on entend par « détection des infractions » :
>
> a) le fait de déterminer par qui, dans quel but, par quel moyen et, de manière générale, dans quelles circonstances une infraction a été commise ; et
>
> b) le fait d'appréhender la personne qui a commis une infraction ;
>
> et toute référence dans la présente loi à la prévention ou à la détection des infractions graves doit se comprendre en ce sens (...) »

65. L'article 6 disposait qu'au sein des services de renseignement, seul le Directeur général du MI5, le Chef du MI6 et le Directeur du GCHQ pouvaient solliciter un mandat d'interception.

66. Les articles 5 et 6 s'appliquaient à deux catégories de mandats d'interception, à savoir le mandat ciblé visé à l'article 8 § 1, et le mandat non ciblé visé à l'article 8 § 4.

67. En vertu de l'article 9 de la RIPA, un mandat émis dans l'intérêt de la sécurité nationale ou pour la sauvegarde de la prospérité économique du Royaume-Uni était valable six mois, et un mandat émis aux fins de la détection des infractions graves était valable trois mois. À tout moment avant l'expiration de ces délais, le ministre compétent pouvait renouveler le mandat (pour la même durée) s'il estimait qu'il demeurait nécessaire pour l'un des motifs visés à l'article 5 § 3. Il devait au contraire l'annuler s'il estimait qu'il n'était plus nécessaire pour l'un des motifs visés à l'article 5 § 3.

68. En vertu de l'article 5 § 6, l'opération autorisée par un mandat d'interception couvrait l'interception de communications non indiquées dans le mandat si cette interception était nécessaire pour l'accomplissement d'actes que le mandat exigeait ou autorisait expressément, ainsi que l'obtention des données de communication associées.

69. L'article 21 § 4 définissait ainsi les « données de communication » :

> a) toutes données de trafic comprises dans une communication ou jointes à celle-ci (par l'expéditeur ou non) aux fins de tout service postal ou système de télécommunication au moyen duquel elle est ou pourrait être transmise ;

b) toute information qui ne comprend aucun passage du contenu de la communication (à l'exception des informations relevant de l'alinéa a) ci-dessus) et qui concerne l'utilisation faite par toute personne :

i. de tout service postal ou service de télécommunication ;

ii. de toute partie d'un système de télécommunication dans le cadre de la fourniture à toute personne ou de l'utilisation par toute personne de tout service de télécommunication ;

c) toute information ne relevant pas des alinéas a) ou b) ci-dessus détenue ou obtenue par une personne qui fournit un service postal ou un service de télécommunication à l'égard des personnes à qui elle fournit le service. »

70. Le code de conduite de mars 2015 sur l'acquisition et la divulgation de données de communication (*Acquisition and Disclosure of Communications Data Code of Practice* – « le code de conduite sur l'acquisition de données de communication ») désignait respectivement ces trois catégories par les expressions « données de trafic », « informations sur l'utilisation des services » et « informations relatives à l'abonné ». L'article 21 § 6 de la RIPA précisait que les « données de trafic » étaient des données qui identifiaient la personne, le matériel, le lieu ou l'adresse vers ou depuis lesquels les communications étaient acheminées, ainsi que les informations relatives aux fichiers ou programmes informatiques ouverts ou utilisés lors de l'envoi ou de la réception d'une communication.

71. Selon l'article 20 de la RIPA, les « données de communication associées » aux communications interceptées pendant leur transmission par un service postal ou un système de télécommunication englobaient toutes les données de communication « obtenues au moyen de l'interception ou dans le cadre de celle-ci » et « relatives à la communication, à l'expéditeur ou à la personne à laquelle la communication [était] parvenue ou devait parvenir ».

2. Les mandats : l'article 8 § 4 de la RIPA

a) Autorisation

72. L'« interception en masse » de communications se faisait sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA. Les paragraphes 4 et 5 de l'article 8 autorisaient le ministre compétent à émettre un mandat aux fins de « l'interception de communications extérieures au cours de leur transmission par un système de télécommunication ».

73. Lorsqu'il émettait un mandat en vertu de l'article 8 § 4 de la RIPA, le ministre compétent devait aussi établir un certificat décrivant les éléments interceptés qu'il estimait nécessaire d'examiner et précisant que cet examen était nécessaire pour les motifs énoncés à l'article 5 § 3 (c'est-à-dire dans l'intérêt de la sécurité nationale, aux fins de la prévention ou de la détection des infractions graves, ou pour la sauvegarde de la prospérité économique du Royaume-Uni, (dans la mesure où celle-ci relevait aussi de l'intérêt de la

sécurité nationale, voir les articles 3.5 et 6.11 du code de conduite en matière d'interception de communication reproduits au paragraphe 96 ci-dessous)).

b) Les communications « extérieures »

74. Selon l'article 20 de la RIPA, une « communication extérieure » était « une communication envoyée ou reçue hors des îles Britanniques ».

75. Dans le cadre de l'affaire *Liberty*, le Directeur général de l'OSCT, Charles Farr, a indiqué qu'un échange des courriers électroniques entre deux personnes se trouvant au Royaume-Uni constituait une « communication intérieure » même si le service de messagerie électronique était hébergé sur un serveur situé aux États-Unis, mais que cette communication pouvait se trouver « accidentellement prise dans les filet » d'une interception réalisée sur la base d'un mandat ciblant des communications extérieures. Il a précisé par ailleurs que la connexion d'une personne se trouvant au Royaume-Uni à un moteur de recherche étranger constituait une communication extérieure, de même que la mise en ligne d'un message public (tel qu'un « tweet » ou un changement de statut Facebook) par une personne se trouvant au Royaume-Uni, sauf si tous les destinataires du message se trouvaient eux-mêmes dans les îles Britanniques.

76. Lorsqu'il a déposé devant la commission parlementaire sur le renseignement et la sécurité en octobre 2014, le ministre des Affaires étrangères et du Commonwealth a indiqué ceci :

> « Pour ce qui est des courriers électroniques, si l'expéditeur, le destinataire ou les deux se trouvent à l'étranger, il s'agit d'une communication extérieure.
>
> Pour ce qui est de la navigation sur Internet, si un individu consulte le site web du Washington Post, il « communique » avec un serveur web situé à l'étranger, et il s'agit donc d'une communication extérieure.
>
> Pour ce qui est des médias sociaux, si un individu met en ligne quelque chose sur Facebook, étant donné que le serveur web se trouve à l'étranger, il s'agit d'une communication extérieure.
>
> Pour ce qui est du stockage de données dans le « Cloud » (par exemple, des fichiers versés sur Dropbox), il s'agit là encore de communications extérieures, car ces données sont envoyées sur un serveur web situé à l'étranger. »

3. Les garanties spécifiques posées par la RIPA

a) L'article 15

77. Le premier paragraphe l'article 15 de la RIPA imposait au ministre compétent l'obligation de veiller, pour tous les mandats d'interception, à la mise en place des procédures qu'il estimait nécessaires pour assurer le respect des exigences posées aux paragraphes 2 et 3 du même article quant aux éléments interceptés et aux données de communication associées.

S’agissant des mandats appelant l’établissement d’un certificat en vertu de l’article 8 § 4, le ministre devait également veiller au respect des exigences formulées à l’article 16.

78. Le paragraphe 2 de l’article 15 était ainsi libellé :

> « Il est satisfait aux exigences posées au présent paragraphe en ce qui concerne les éléments interceptés et les données de communication associées si chacun des facteurs ci-dessous est limité au minimum nécessaire pour la réalisation des buts autorisés :
>
> a) le nombre de personnes auxquelles l’un quelconque des éléments interceptés ou des données associées est divulgué ou accessible,
>
> b) la mesure dans laquelle l’un quelconque des éléments interceptés ou des données associées est divulgué ou accessible,
>
> c) la mesure dans laquelle l’un quelconque des éléments interceptés ou des données associées est copiée, et
>
> d) le nombre de copies réalisées. »

79. Le paragraphe 3 de l’article 15 se lisait ainsi:

> « Il est satisfait aux exigences posées au présent paragraphe en ce qui concerne les éléments interceptés et les données de communication associées si chaque copie faite de l’un quelconque des éléments interceptés ou des données associées est détruite (si ce n’a déjà été fait) dès qu’il n’y a plus de motif rendant sa conservation nécessaire dans l’un des buts autorisés. »

80. En vertu du paragraphe 4 de l’article 15, une chose était nécessaire dans l’un des buts autorisés si et seulement si elle restait ou était susceptible de devenir nécessaire au sens de l’article 5 § 3 (c’est-à-dire dans l’intérêt de la sécurité nationale, aux fins de la prévention ou de la détection des infractions graves, pour la sauvegarde de la prospérité économique du Royaume-Uni – dans la mesure où celle-ci relevait aussi de l’intérêt de la sécurité nationale, voir les paragraphes 3.5 et 6.11 du code de conduite en matière d’interception de communication reproduits au paragraphe 96 ci-dessous – ou pour donner effet aux dispositions d’un accord d’entraide internationale) ; si elle était nécessaire pour faciliter l’accomplissement de l’une quelconque des missions d’interception du ministre ; si elle était nécessaire pour faciliter l’accomplissement de l’une quelconque des missions du Commissaire à l’interception des communications ou de l’IPT ; si elle était nécessaire pour qu’une personne en charge de poursuites pénales dispose des informations dont elle avait besoin pour déterminer ce qu’elle était tenue de faire en vertu de son obligation d’assurer l’équité de la procédure ; ou si elle était nécessaire pour l’exécution de toute obligation imposée à toute personne par la législation relative aux archives publiques.

81. En vertu du paragraphe 5 de l’article 15, les mesures que le ministre compétent estimait nécessaires pour que chaque copie d’éléments interceptés ou de données associées soit stockée de manière sécurisée pendant toute la durée de sa conservation devaient figurer parmi les procédures mises en place pour assurer le respect du paragraphe 2.

82. Le paragraphe 6 de l'article 15 énonçait qu'il n'était pas impératif que les procédures visées au premier paragraphe de l'article 15 garantissent le respect des exigences posées aux paragraphes 2 et 3 s'agissant des originaux et des copies des éléments interceptés et des données de communication associées remis aux autorités d'un pays ou territoire non britannique. En revanche, ces procédures devaient garantir, pour tous les mandats d'interception, que les originaux et les copies de ces éléments et données ne soient remis aux autorités d'un pays ou territoire non britannique que s'il était satisfait aux exigences posées au paragraphe 7, lequel était ainsi libellé :

> « Il est satisfait aux exigences posées au présent paragraphe lorsqu'un mandat est établi s'il apparaît au ministre compétent :
>
> a) que des exigences correspondant à celles énoncées aux paragraphes 2 et 3 s'appliqueront, éventuellement dans la mesure jugée appropriée par le ministre, à tous les éléments interceptés et toutes les données de communication associées dont l'original ou une copie sont remis aux autorités en question ; et
>
> b) que sont en vigueur des restrictions qui empêcheraient, éventuellement dans la mesure jugée appropriée par le ministre, que soit réalisée, dans le cadre ou aux fins d'une procédure menée hors du Royaume-Uni, ou à l'occasion d'une telle procédure, une quelconque opération aboutissant à une divulgation qui serait interdite au Royaume-Uni en vertu de l'article 17. »

83. L'article 17 de la RIPA posait un principe général d'interdiction de toute production de preuve, communication d'informations ou autre démarche liée à une procédure judiciaire et susceptible d'aboutir à la divulgation du contenu d'une communication interceptée ou des données de communication associées.

b) L'article 16

84. L'article 16 de la RIPA prévoyait des garanties supplémentaires applicables à l'interception de communications « extérieures » sur la base d'un mandat émis en vertu de l'article 8 § 4. Le premier paragraphe de cet article disposait que les éléments interceptés ne pouvaient être lus, consultés ou écoutés que par les personnes qui y avaient accès en vertu du mandat, et dans la stricte mesure où, premièrement, ils avaient fait l'objet d'un certificat attestant que leur examen était nécessaire conformément à l'article 5 § 3 et, deuxièmement, ils relevaient du paragraphe 2. En vertu de l'article 20, l'expression « éléments interceptés » devait être comprise comme désignant le contenu de toute communication interceptée dans le cadre du mandat.

85. Le paragraphe 2 de l'article 16 était ainsi libellé :

« Sous réserve des paragraphes 3 et 4 du présent article, les éléments interceptés ne relèvent du présent paragraphe que dans la mesure où ils sont sélectionnés pour être lus, consultés ou écoutés sur une base autre qu'un facteur :

a) lié à une personne dont on sait qu'elle se trouve actuellement dans les îles Britanniques ; et

b) dont le but ou l'un des buts est la découverte d'éléments contenus dans les communications que cette personne envoie ou qui lui sont destinées. »

86. En vertu du paragraphe 3 de l'article 16, des éléments interceptés relevaient du paragraphe 2 même s'ils avaient été sélectionnés en fonction de l'un des facteurs visés à ce paragraphe dès lors, premièrement, qu'ils avaient fait l'objet d'un certificat du ministre compétent aux fins de l'article 8 § 4 attestant que l'examen d'éléments sélectionnés en fonction de facteurs liés à la personne concernée était nécessaire pour l'un des motifs prévus à l'article 5 § 3 et, deuxièmement, qu'ils ne concernaient que des communications envoyées pendant une période ne dépassant pas la durée maximale autorisée, précisée dans le certificat.

87. En vertu du paragraphe 3A de l'article 16, la « durée maximale autorisée » était de :

« a) six mois pour les éléments dont l'examen est certifié nécessaire dans l'intérêt de la sécurité nationale aux fins de l'article 8 § 4 ; et

b) trois mois dans tous les autres cas. »

88. En vertu du paragraphe 4 de l'article 16, les éléments interceptés relevaient aussi du paragraphe 2 même s'ils avaient été sélectionnés en fonction de l'un des facteurs visés à ce paragraphe lorsque la personne à laquelle le mandat avait été délivré estimait, sur la base de motifs raisonnables, que les circonstances les faisaient relever dudit paragraphe, et lorsque les conditions de sélection de ces éléments énoncées au paragraphe 5 étaient réunies.

89. Le paragraphe 5 de l'article 16 était ainsi libellé :

« Ces conditions de sélection des éléments sont réunies si :

a) il apparaît à la personne à laquelle le mandat a été délivré qu'il y a eu un changement pertinent de circonstances qui, sans le paragraphe 4 b), empêcherait les éléments interceptés de relever du paragraphe 2 ;

b) depuis cette découverte, une autorisation écrite de lire, consulter ou écouter les éléments a été donnée par un officier supérieur ; et

c) la sélection est faite avant la fin de la période d'autorisation. »

90. En vertu du paragraphe 5A de l'article 16, la « période d'autorisation » désignait :

« a) pour ce qui est des éléments dont l'examen est certifié nécessaire dans l'intérêt de la sécurité nationale aux fins de l'article 8 § 4, la période qui s'achève à l'issue du cinquième jour ouvrable après qu'il est apparu à la

personne à laquelle le mandat a été délivré qu'il y a eu un changement de circonstances visé au paragraphe 5 a) ; et

b) dans tous les autres cas, la période qui s'achève à l'issue du premier jour ouvrable après qu'il est apparu à cette personne qu'il y a eu un tel changement. »

91. Le paragraphe 6 de l'article 16 précisait que l'expression « changement pertinent de circonstances » signifiait qu'il apparaissait soit que l'individu concerné était entré sur les îles Britanniques soit que la personne à laquelle le mandat avait été délivré avait cru à tort que l'individu se trouvait hors des îles Britanniques.

92. Lorsqu'il a déposé devant la commission parlementaire sur le renseignement et la sécurité en octobre 2014, le ministre des Affaires étrangères et du Commonwealth a expliqué ceci :

« Lorsqu'un analyste sélectionne pour examen des communications qui ont été interceptées sur la base d'un mandat émis en vertu de l'article 8 § 4, la forme de communication utilisée par l'individu est sans importance, de même que le fait que ses autres communications soient ou non stockées sur un serveur de courrier électronique dédié ou dans le « Cloud » au Royaume-Uni, aux États-Unis ou ailleurs (au demeurant, en pratique, les utilisateurs de services sur le « Cloud » ne savent pas où leurs données sont stockées). Si l'on sait que l'individu se trouve dans les îles Britanniques, il est interdit de rechercher ses communications en utilisant son nom, son adresse de courrier électronique ou un autre identifieur personnel. »

4. Le code de conduite en matière d'interception de communications

93. L'article 71 de la RIPA prévoyait que le ministre compétent devait adopter des codes de conduite pour la mise en œuvre des pouvoirs et obligations découlant de la loi. Les projets de code de conduite devaient être déposés devant le Parlement et étaient des documents publics. Ils ne pouvaient entrer en vigueur qu'en vertu d'une ordonnance du ministre, que celui-ci ne pouvait prendre que si le projet d'ordonnance avait été déposé devant le Parlement et approuvé par une résolution de chaque chambre.

94. En vertu de l'article 72 § 1 de la RIPA, toute personne exerçant un pouvoir ou exécutant une obligation en matière d'interception de communications devait tenir compte des dispositions pertinentes du code de conduite correspondant. En vertu de l'article 72 § 4, les tribunaux pouvaient, si les circonstances le justifiaient, prendre en compte les dispositions du code de conduite.

95. Le code de conduite en matière d'interception de communications a été adopté en vertu de l'article 71 de la RIPA. La version de ce code en vigueur à l'époque pertinente datait de 2016.

96. En ses parties pertinentes, ce code prévoyait ceci :

« 3.2. Un nombre limité de personnes peuvent demander un mandat d'interception, ou déléguer le pouvoir de faire cette demande. Ces personnes sont :

- le Directeur général du *Security Service* [MI5, sécurité intérieure].

- le Chef du *Secret Intelligence Service* [MI6, renseignement extérieur].
- le Directeur du *Government Communications Headquarters* (GCHQ).
- le Directeur général du *National Crime Agency* [service de lutte contre la criminalité] (le NCA gère les interceptions pour le compte des forces de l'ordre en Angleterre et au Pays-de-Galles).
- l'Inspecteur général de la Police écossaise.
- le *Commissioner of the Police of the Metropolis* [Préfet de police du Grand Londres] (le service de lutte contre le terrorisme de la *Metropolitan Police* [police de Londres] gère les interceptions pour le compte des cellules de lutte contre le terrorisme, des sections spécialisées et de certaines cellules spécialisées de la police en Angleterre et aux Pays-de-Galles).
- l'Inspecteur général de la Police d'Irlande du Nord.
- les *Commissioners of Her Majesty's Revenue & Customs* (HMRC) [administrateurs généraux du service des recettes et douanes].
- le Chef du *Defence Intelligence* [renseignement militaire].
- toute personne qui, en vertu d'un accord d'entraide internationale, est l'autorité compétente d'un pays ou territoire non britannique.

3.3. Toute demande faite au nom de l'une des personnes susmentionnées doit être soumise par un titulaire d'une charge relevant de la Couronne.

3.4. Tous les mandats d'interception sont émis par le ministre compétent. Même en cas d'application de la procédure d'urgence, le ministre doit autoriser en personne la délivrance du mandat, même si celui-ci est signé par un officier supérieur.

Nécessité et proportionnalité

3.5. L'obtention d'un mandat dans les conditions définies par la RIPA ne justifie l'ingérence dans le droit d'un individu au titre de l'article 8 de la Convention européenne des droits de l'homme (le droit à la vie privée) que constitue l'interception autorisée que si celle-ci est nécessaire et proportionnée. Cela découle de la RIPA elle-même, d'abord parce qu'elle énonce que la délivrance d'un mandat doit être considérée comme nécessaire par le ministre compétent pour l'un au moins des motifs des motifs légaux suivants :

- l'intérêt de la sécurité nationale ;
- la prévention ou de la détection des infractions graves ;
- la sauvegarde de la prospérité économique du Royaume-Uni, dans la mesure où celle-ci relève aussi de l'intérêt de la sécurité nationale.

3.6. Ces buts sont énoncés à l'article 5 § 3 de la RIPA. Celle-ci oblige aussi le ministre compétent à rechercher si l'interception est proportionnée au but qu'elle poursuit. Pour évaluer la proportionnalité de l'interception, il faut toujours mettre en balance la gravité de l'intrusion dans la vie privée ou de l'atteinte aux biens du sujet visé par l'opération (ou de toute autre personne que celle-ci affecterait) et la nécessité de l'activité envisagée, du point de vue de l'enquête, du point de vue opérationnel ou en termes de capacité. Le mandat ne constituera pas une mesure proportionnée s'il est excessif eu égard à l'ensemble des circonstances de l'espèce. Chaque action autorisée doit viser à apporter un bénéfice à l'enquête ou à l'opération et ne pas être disproportionnée au but visé ni arbitraire. Par exemple, une menace potentielle pour la

sécurité nationale ne peut à elle seule rendre proportionnées les actions les plus intrusives. Aucune ingérence ne peut être considérée comme proportionnée s'il est raisonnablement possible d'obtenir par d'autres moyens moins intrusifs les informations qu'elle vise à recueillir.

3. RÈGLES GÉNÉRALES RELATIVES À L'INTERCEPTION SUR MANDAT

(...)

3.7. Pour s'assurer de la proportionnalité de la mesure, il faut donc :

- mettre en balance l'ampleur et la portée de l'ingérence envisagée avec le but recherché ;
- expliquer comment et pourquoi les méthodes à adopter causeront l'intrusion la plus réduite possible pour le sujet et pour les tiers ;
- rechercher, après examen de toutes les autres possibilités raisonnables, si la mesure envisagée constitue une application appropriée de la loi et un moyen raisonnable d'obtenir le résultat nécessaire ;
- préciser, autant qu'il est raisonnablement possible de le faire, quelles autres méthodes ont été envisagées et soit n'ont pas été mises en œuvre soit ont été employées mais ont été jugées insuffisantes pour parvenir aux objectifs opérationnels visés sans l'adjonction des éléments dont l'interception est envisagée.

(...)

Durée des mandats d'interception

3.18. Les mandats d'interception émis pour un motif concernant les infractions graves sont valables pour une période initiale de trois mois. Les mandats d'interception émis pour un motif concernant la sécurité nationale ou la sauvegarde de la prospérité économique du pays sont valables pour une période initiale de six mois. Les mandats émis dans le cadre de la procédure d'urgence (quel que soit le motif) sont valables pendant cinq jours ouvrables à compter de leur date d'émission, à moins qu'ils ne soient renouvelés par le ministre compétent.

3.19. Le renouvellement prolonge de trois mois les mandats émis pour un motif concernant les infractions graves. Il prolonge de six mois les mandats émis pour un motif concernant la sécurité nationale ou la sauvegarde de la prospérité économique du pays. Ces périodes commencent à courir à compter de la date de l'acte de renouvellement.

3.20. Lorsque des modifications sont apportées à un mandat d'interception, la date d'expiration du mandat demeure inchangée. Toutefois, lorsque la modification s'inscrit dans le cadre de la procédure d'urgence, l'acte de modification expire cinq jours ouvrables après sa date d'émission, à moins qu'il ne soit renouvelé conformément à la procédure ordinaire.

3.21. Lorsqu'un changement de circonstances amène l'agence interceptrice à considérer qu'il n'est plus nécessaire, proportionné ou matériellement possible que le mandat demeure en vigueur, celle-ci doit recommander au ministre compétent d'annuler le mandat par une décision d'effet immédiat.

(...)

4. RÈGLES SPÉCIALES RELATIVES À L'INTERCEPTION SUR MANDAT

Intrusion collatérale

4.1. Il faut tenir compte du risque d'ingérence dans la vie privée d'individus qui ne sont pas visés par l'interception, en particulier lorsque peuvent être concernées des communications portant sur des sujets religieux, médicaux, journalistiques ou soumis au secret professionnel, ou des communications entre un parlementaire et une autre personne relatives aux affaires de la circonscription du parlementaire, ou des communications entre un parlementaire et un lanceur d'alerte. La demande de mandat d'interception doit préciser s'il y a un risque que l'interception porte atteinte à la vie privée de tiers (intrusion collatérale). La personne sollicitant le mandat d'interception doit aussi envisager des mesures, y compris l'utilisation de systèmes automatisés, visant à réduire l'ampleur de l'intrusion collatérale. Lorsqu'il est possible de le faire, la demande doit préciser quelles sont ces mesures. Le ministre compétent prend en compte ces circonstances et ces mesures lorsqu'il examine les demandes de mandat relevant de l'article 8 § 1 de la RIPA. Si, au cours d'une opération d'interception, des individus autres que celui visé par l'autorisation sont identifiés comme devant eux-mêmes faire l'objet d'une enquête, il faut envisager de demander des mandats distincts pour les individus en question.

Informations confidentielles

4.2. Il faut aussi accorder une attention particulière aux cas où le sujet de l'interception peut raisonnablement s'attendre à ce que ses communications bénéficient d'un degré élevé de confidentialité, et aux situations dans lesquelles des informations confidentielles sont en cause. Il en va ainsi des communications portant sur des éléments couverts par le secret professionnel des avocats, des communications pouvant porter sur des éléments journalistiques confidentiels, des interceptions pouvant avoir trait à des communications échangées entre un individu et un professionnel de la santé ou un ministre du culte au sujet de la santé ou de la spiritualité de l'individu, et des communications qui concerneraient des échanges entre un parlementaire et une autre personne relativement aux affaires de la circonscription.

4.3. Les éléments journalistiques confidentiels comprennent les éléments obtenus ou créés à des fins d'activité journalistique et détenus sur la foi d'un engagement de confidentialité, ainsi que les communications aboutissant à l'obtention d'informations destinées à des activités journalistiques et détenues sur la foi d'un tel engagement. Voir aussi les paragraphes 4.26 et 4.28 à 4.31, où sont énoncées des garanties supplémentaires applicables aux éléments journalistiques confidentiels.

(...)

Communications portant sur des éléments journalistiques confidentiels, des informations personnelles confidentielles ou des communications échangées entre un parlementaire et une autre personne relativement aux affaires de la circonscription

4.26. L'interception de communications portant sur des éléments journalistiques confidentiels, des informations personnelles confidentielles, ou des échanges entre un parlementaire et une autre personne au sujet des affaires de la circonscription appellent également une attention particulière. La notion d'éléments journalistiques confidentiels est définie au paragraphe 4.3. Les informations personnelles confidentielles sont des informations reçues à titre confidentiel qui concernent un individu (vivant ou mort) qu'elles permettent d'identifier et qui ont trait à sa santé physique ou mentale ou à des conseils spirituels. Ces informations peuvent figurer dans des communications orales comme dans des communications écrites. Elles sont

reçues à titre confidentiel si elles ont été obtenues sur la foi d'un engagement explicite ou implicite à cet effet ou si elles sont soumises à une restriction de divulgation ou à une obligation de confidentialité prévues par la législation en vigueur. Parmi ces informations figurent notamment les consultations entre un professionnel de la santé et un patient, ainsi que les éléments figurant dans le dossier médical de celui-ci.

(...)

4.28. Lorsque la mesure envisagée vise à permettre l'acquisition d'informations personnelles confidentielles, les motifs sur lesquels elle repose doivent être clairement précisés et sa nécessité et sa proportionnalité spécifiques soigneusement soupesées. Si l'acquisition d'informations personnelles confidentielles est probable mais non recherchée, toutes les possibilités d'atténuation de ce risque doivent être envisagées et, s'il n'en existe aucune, il faut réfléchir à la nécessité de mettre en place des procédures spéciales pour le traitement de ces informations au sein de l'agence interceptrice.

4.29. Les éléments identifiés comme étant des informations confidentielles ne peuvent être conservés que si pareille mesure est nécessaire et proportionnée dans un ou plusieurs des buts autorisés par l'article 15 § 4 [de la RIPA]. Ils doivent être détruits de manière sécurisée lorsque leur conservation n'est plus nécessaire au regard de ces buts. S'ils sont conservés, des systèmes de gestion de l'information adéquats garantissant que leur conservation demeure nécessaire et proportionnée au regard des buts autorisés par la loi doivent être mis en place.

4.30. Lorsque des informations confidentielles sont conservées ou transmises à un organe externe, il faut prendre des mesures raisonnables pour signaler leur caractère confidentiel. En cas de doute quant à la licéité du traitement ou de la transmission envisagés d'informations confidentielles, un conseiller juridique de l'agence interceptrice concernée doit être consulté avant la poursuite de la transmission.

4.31. Toute conservation d'informations confidentielles doit être signalée au Commissaire à l'interception des communications aussitôt qu'il est raisonnablement possible de le faire, selon les modalités convenues avec lui. Tous les éléments conservés doivent être mis à la disposition du Commissaire à sa demande.

4.32. Les garanties énoncées aux paragraphes 4.28 à 4.31 s'appliquent également à tous les éléments relevant de l'article 8 § 4 de la RIPA (voir le chapitre 6) qui sont sélectionnés pour examen et qui constituent des informations confidentielles.

(...)

6. MANDATS D'INTERCEPTION (ARTICLE 8 § 4 DE LA RIPA)

6.1. La présente section s'applique à l'interception de communications extérieures sur la base d'un mandat émis en vertu de l'article 8 § 4 de la RIPA.

6.2. Contrairement aux mandats relevant de l'article 8 § 1, les mandats relevant de l'article 8 § 4 ne doivent pas obligatoirement désigner nommément ou décrire le sujet de l'interception ou les lieux auxquels doit s'appliquer l'interception. L'article 8 § 4 n'impose pas non plus de limite expresse au nombre de communications extérieures pouvant être interceptées. Par exemple, toutes les communications transmises par un canal ou un câble donné, ou acheminées par un fournisseur de services de communication donné peuvent en principe faire légalement l'objet d'une autorisation d'interception dès lors qu'il est satisfait aux exigences des paragraphes 4 et 5 de l'article 8. En effet, les interceptions réalisées en vertu de l'article 8 § 4 sont un moyen d'obtenir des renseignements, alors que les interceptions réalisées en vertu de

l'article 8 § 1 sont principalement un outil d'enquête, utilisé lorsqu'un sujet d'interception donné a été identifié.

6.3. La responsabilité d'émettre des mandats d'interception en vertu de l'article 8 § 4 de la RIPA incombe au ministre compétent. Lorsque celui-ci émet un mandat en vertu de ce paragraphe, le mandat doit être accompagné d'un certificat. Ce certificat garantit qu'un processus de sélection sera appliqué aux éléments interceptés afin que seuls les éléments qu'il décrit puissent être examinés par un être humain. Si le principe de proportionnalité et les termes du certificat interdisent que les éléments interceptés soient sélectionnés pour être lus, consultés ou écoutés, personne ne peut les lire, les consulter ou les écouter.

Les interceptions réalisées en vertu de l'article 8 § 4 de la RIPA en pratique

6.4. Les mandats émis en vertu de l'article 8 § 4 de la RIPA autorisent l'interception de communications extérieures. Lorsqu'un mandat émis en vertu de l'article 8 § 4 aboutit à l'acquisition d'un gros volume de communications, l'agence interceptrice a généralement recours à un processus de filtrage visant à écarter automatiquement les communications qui sont peu susceptibles de présenter un intérêt du point de vue du renseignement. Les personnes autorisées de cette agence peuvent ensuite appliquer des critères de recherche pour sélectionner les communications susceptibles de présenter un intérêt conformément au certificat émis par le ministre compétent. Avant qu'une personne autorisée de l'agence interceptrice ne puisse accéder à une communication, elle doit expliquer pourquoi cet accès est nécessaire au regard de l'un des motifs énoncés dans le certificat accompagnant le mandat, et pourquoi il constituerait une mesure proportionnée au but visé dans le cas d'espèce. Ce processus fait l'objet d'un contrôle interne et est soumis à la supervision externe du Commissaire à l'interception des communications. Lorsque le ministre compétent le juge nécessaire, il peut autoriser la sélection de communications d'un individu dont on sait qu'il se trouve dans les îles Britanniques. En l'absence d'une telle autorisation, la personne autorisée ne peut pas sélectionner de telles communications.

Définition des communications extérieures

6.5. Selon la RIPA, les communications extérieures sont celles qui sont envoyées ou reçues hors des îles Britanniques, ainsi que celles qui sont envoyées et reçues hors des îles Britanniques, qu'elles transitent ou non par les îles Britanniques au cours de leur transmission. Elles ne comprennent pas les communications envoyées et reçues dans les îles Britanniques, même si ces communications transitent hors des îles Britanniques. Par exemple, un courrier électronique envoyé par une personne de Londres à une personne de Birmingham est une communication intérieure et non une communication extérieure aux fins de l'article 20 de la RIPA, indépendamment du fait qu'elle transite ou non par des adresses IP situées hors des îles Britanniques, car l'expéditeur et le destinataire se trouvent tous deux dans les îles Britanniques.

Interception de communications non extérieures dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA

6.6. Il ressort clairement de l'article 5 § 6 a) de la RIPA que l'opération autorisée par un mandat émis en vertu de l'article 8 § 4 peut, en principe, comprendre l'interception de communications non extérieures dans la mesure nécessaire à l'interception de communications extérieures relevant du mandat.

6.7. Lorsqu'elle procède à une interception dans le cadre d'un mandat émis en vertu de l'article 8 § 4, l'agence interceptrice doit utiliser sa connaissance de l'acheminement des communications internationales ainsi que des études régulières des différentes liaisons de communication pour identifier les canaux de transmission

les plus susceptibles de contenir des communications extérieures qui répondent à la description des éléments sur lesquels porte le certificat ministériel relevant de l'article 8 § 4. Elle doit aussi intercepter les données de manière à limiter la collecte de communications non extérieures au minimum compatible avec le but assigné à l'interception des communications extérieures visées.

Demande de délivrance d'un mandat en vertu de l'article 8 § 4 de la RIPA

6.8. La demande de mandat est adressée au ministre compétent. Une fois émis, le mandat d'interception est délivré à la personne qui en a fait la demande. Le but du mandat doit en général correspondre à une ou plusieurs des priorités en matière de renseignement fixées par le Conseil de sécurité nationale [*National Security Council*] (NSC).

6.9. Avant d'être déposée, chaque demande fait l'objet d'un contrôle au sein de l'agence dont elle émane. Dans ce cadre, elle est examinée par plusieurs personnes, qui vérifient si elle vise un but relevant de l'article 5 § 3 de la RIPA et si l'interception envisagée est nécessaire et proportionnée au but visé.

6.10. Le demandeur doit conserver une copie de la demande. Chaque demande doit renfermer les informations suivantes :

- le contexte de l'opération en question :
  - description des communications à intercepter, informations relatives au(x) fournisseur(s) de services de communication et évaluation de la faisabilité de l'opération, le cas échéant ; et
  - description de l'opération à autoriser, laquelle doit être circonscrite à l'interception de communications extérieures, ou les démarches (y compris l'interception d'autres communications non indiquées expressément dans le mandat, comme le permet l'article 5 § 6 a) de la RIPA) nécessaires pour mener à bien l'activité autorisée ou exigée par le mandat, et l'obtention des données de communication associées.
- le certificat régissant l'examen des éléments interceptés ;
- un exposé des motifs pour lesquels l'interception est jugée nécessaire dans l'un ou plusieurs des buts énoncés à l'article 5 § 3 [de la RIPA] ;
- un exposé des motifs pour lesquels l'opération que le mandat doit autoriser est proportionnée au but visé ;
- en cas de demande urgente, les justificatifs correspondants ;
- l'assurance que les éléments interceptés ne seront lus, consultés ou écoutés que dans la mesure où ils font l'objet d'un certificat et répondent aux conditions énoncées aux articles 16 § 2 à 16 § 6 de la RIPA ; et
- l'assurance que tous les éléments interceptés seront traités dans le respect des garanties posées aux articles 15 et 16 de la RIPA (voir les paragraphes 7.2 et 7.10).

Délivrance d'un mandat relevant de l'article 8 § 4 de la RIPA

6.11. Avant de délivrer un mandat en vertu de l'article 8 § 4 de la RIPA, le ministre compétent doit s'assurer que cette mesure est nécessaire :

- dans l'intérêt de la sécurité nationale ;

- aux fins de la prévention ou de la détection des infractions graves ; ou
- aux fins de la sauvegarde de la prospérité économique du Royaume-Uni dans la mesure où celle-ci relève aussi de l'intérêt de la sécurité nationale.

6.12. Le ministre ne peut émettre un mandat d'interception aux fins de la sauvegarde de la prospérité économique du Royaume-Uni (article 5 § 3 c) de la RIPA) que s'il lui apparaît que la situation en cause relève de l'intérêt de la sécurité nationale. Il ne peut délivrer un mandat en vertu de l'article 5 § 3 c) en l'absence d'un lien direct entre la prospérité économique du Royaume-Uni et la sécurité nationale. Toute demande de délivrance d'un mandat sur le fondement de l'article 5 § 3 c) doit donc préciser quelles sont les circonstances faisant entrer en jeu la sécurité nationale.

6.13. Le ministre doit aussi s'assurer que l'intervention autorisée par le mandat est proportionnée au but visé (article 5 § 2 b)). Lorsqu'il examine la nécessité et la proportionnalité de la mesure, il doit se demander si les informations recherchées pourraient raisonnablement être obtenues par d'autres moyens (article 5 § 4).

6.14. L'émission d'un mandat de ce type doit être accompagnée d'un certificat par lequel le ministre confirme qu'il estime que l'examen des éléments interceptés est nécessaire dans l'un ou plusieurs des buts relevant de l'article 5 § 3. Le certificat prévu par la loi vise à garantir que les éléments interceptés feront l'objet d'une sélection de manière à ce que seuls les éléments qu'il décrit puissent être examinés par un être humain. Tous les certificats doivent répondre aux « Priorités en matière de collecte de renseignement » établies par le NSC à l'intention des agences de renseignement. Par exemple, un certificat peut prévoir l'examen d'éléments renfermant des renseignements en matière de terrorisme (au sens de la loi de 2000 sur le terrorisme [*Terrorism Act 2000*]) ou de stupéfiants réglementés (au sens de la loi de 1971 relative à l'abus des drogues [*Misuse of Drugs Act 1971*]). Toutes les modifications éventuellement apportées à la description des éléments indiqués dans le certificat doivent être soumises au Commissaire à l'interception des communications.

6.15. Il incombe au ministre compétent de veiller à l'instauration de procédures visant à garantir que seuls les éléments dont l'examen a été certifié nécessaire dans un but relevant de l'article 5 § 3 de la RIPA et répondant aux conditions énoncées à l'article 16 § 2 ou à l'article 16 § 6 soient en pratique lus, consultés ou écoutés. Le Commissaire à l'interception des communications est tenu de s'assurer de l'efficacité de ces procédures.

Délivrance en urgence d'un mandat relevant de l'article 8 § 4 de la RIPA

6.16. L'article 7 § l b) de la RIPA prévoit qu'en cas d'urgence, un mandat peut être délivré sans que le ministre compétent ait été en mesure de le signer. L'interception doit alors avoir été autorisée par le ministre lui-même, mais le mandat peut être signé par un haut responsable, après discussion de l'affaire entre les responsables et le ministre. La RIPA restreint cette procédure aux cas urgents où le ministre a personnellement et expressément autorisé la délivrance du mandat (article 7 § 2 a)), et elle dispose que le mandat doit en faire état (article 7 § 4 a)).

6.17. Un mandat délivré dans le cadre de la procédure d'urgence est valable cinq jours ouvrables à compter de sa date d'émission à moins qu'il ne soit renouvelé par le ministre, auquel cas il expire au bout de trois mois s'il concerne des infractions graves ou de six mois s'il concerne la sécurité nationale ou de la prospérité économique du pays, comme un mandat émis en vertu de l'article 8 § 4 selon la voie ordinaire.

Forme du mandat émis en vertu de l'article 8 § 4 de la RIPA

6.18. Chaque mandat est délivré à la personne qui en a fait la demande. Celle-ci peut ensuite en adresser une copie aux fournisseurs de services de communication qu'il estime aptes à l'aider à la mise en œuvre de l'interception, mais les fournisseurs de services de communication ne reçoivent pas en principe de copie du certificat correspondant. Le mandat doit comprendre les mentions suivantes :

- une description des communications à intercepter ;
- le numéro de référence du mandat ; et
- les nom et qualité des personnes qui pourront modifier le certificat correspondant en cas d'urgence (si cette possibilité est autorisée en vertu de l'article 10 § 7 de la RIPA).

Modification d'un mandat et/ou d'un certificat émis en vertu de l'article 8 § 4 de la RIPA

6.19. Les mandats d'interception et les certificats correspondants peuvent être modifiés selon la procédure prévue à l'article 10 de la RIPA. Les mandats ne peuvent être modifiés que par le ministre compétent ou, en cas d'urgence, par un haut responsable expressément habilité à cette fin par le ministre. En pareil cas, l'acte de modification doit mentionner cette habilitation, et la modification devient caduque cinq jours ouvrables après son émission à moins qu'elle n'ait été approuvée par le ministre.

6.20. Seul le ministre compétent peut modifier un certificat, sauf dans les cas d'urgence où celui-ci peut être modifié par un haut responsable, à condition que ce dernier occupe une fonction qui l'habilite expressément à modifier ce certificat au nom du ministre en vertu de dispositions figurant dans le certificat, ou que le ministre ait expressément autorisé la modification et qu'il en soit fait mention dans l'acte de modification. En pareil cas, la modification devient caduque cinq jours ouvrables après son émission à moins qu'elle n'ait été approuvée par le ministre.

6.21. Lorsque le ministre compétent l'estime nécessaire, le certificat peut être modifié pour autoriser la sélection de communications d'un individu se trouvant dans les îles Britanniques. Le lieu où se trouve l'individu doit être déterminé à l'aide de toutes les informations disponibles. S'il n'est pas possible d'établir ce lieu avec certitude au moyen de ces informations, il faut déterminer de bonne foi, compte tenu des éléments dont on dispose, le lieu où l'individu se trouve vraisemblablement. Si l'on soupçonne fortement qu'un individu se trouve sur le sol britannique, les dispositions énoncées dans le présent paragraphe s'appliquent.

Renouvellement d'un mandat émis en vertu de l'article 8 § 4 de la RIPA

6.22. Avant sa date d'expiration, un mandat peut être renouvelé à tout moment par le ministre compétent. Les demandes de renouvellement doivent être adressées au ministre et comporter un exposé actualisé des points énoncés au paragraphe 6.10 ci-dessus. L'auteur de la demande doit notamment expliquer l'intérêt que revêt l'interception au moment de la demande et les raisons pour lesquelles il considère qu'elle demeure nécessaire dans l'un ou plusieurs des buts relevant de l'article 5 § 3 de la RIPA, et proportionnée au but visé.

6.23. Le ministre compétent peut renouveler le mandat s'il estime que l'interception demeure conforme aux exigences de la RIPA. Si le mandat initial avait été émis pour des motifs relatifs à la prévention des infractions graves, le renouvellement le proroge de trois mois. S'il avait été émis pour des motifs relatifs à la sécurité nationale ou à la prospérité économique du pays, le renouvellement le proroge de six mois. Ces délais commencent à courir à partir de la date de la signature de l'acte de renouvellement.

6.24. Le cas échéant, les fournisseurs de services de communication dont l'assistance avait été requise et qui s'étaient vu adresser une copie du mandat initial doivent recevoir une copie de l'acte de renouvellement du mandat s'ils continuent à fournir une assistance active. L'acte de renouvellement comporte le numéro de référence du ou des mandats qu'il renouvelle.

Annulation d'un mandat

6.25. Si, à quelque moment que ce soit avant l'expiration du mandat d'interception, le ministre compétent estime que celui-ci n'est plus nécessaire dans un but relevant de l'article 5 § 3 de la RIPA, il doit l'annuler. Les agences interceptrices doivent donc vérifier continuellement la nécessité du mandat et avertir le ministre si elles jugent que l'interception n'est plus nécessaire. En pratique, la charge d'annuler le mandat incombe au haut responsable du service ayant émis le mandat au nom du ministre.

6.26. L'acte d'annulation est adressé à la personne (de l'agence interceptrice) à laquelle le mandat avait été délivré. Une copie de l'instrument d'annulation doit être adressée, le cas échéant, à tous les fournisseurs de services de communication qui ont donné effet au mandat au cours des douze derniers mois.

Tenue des dossiers

6.27. Le régime de supervision permet au Commissaire à l'interception des communications d'examiner la demande de mandat sur laquelle repose la décision du ministre compétent, et l'agence interceptrice peut devoir en justifier la teneur. Chaque agence interceptrice doit conserver les éléments suivants pour pouvoir les communiquer au Commissaire à sa demande afin qu'il les examine :

- toutes les demandes de mandat relevant de l'article 8 § 4 de la RIPA et les demandes de renouvellement de ces mandats ;
- tous les mandats et les certificats correspondants et, le cas échéant, les copies des actes de renouvellement ou de modification ;
- en cas de refus d'une demande, les motifs de refus avancés par le ministre ;
- les dates de début et de fin des interceptions.

6.28. Il convient également de tenir un registre des procédures garantissant que seuls les éléments qui ont fait l'objet d'un certificat autorisant leur examen pour un motif prévu à l'article 5 § 3 de la RIPA et qui satisfont aux conditions énoncées aux paragraphes 2 à 6 de l'article 16 combinés à l'article 15 soient en pratique lus, consultés ou écoutés. Les procédures mises en place pour assurer le respect des exigences posées aux paragraphes 2 (maintien au strict minimum de la copie et de la diffusion des éléments interceptés) et 3 (destruction des éléments interceptés) de l'article 15 doivent également être consignées dans un registre. On trouvera plus de détails à ce sujet dans le chapitre « Garanties ».

7. GARANTIES

7.1. Tous les éléments interceptés dans le cadre d'un mandat émis en vertu de l'article 8 § 1 ou de l'article 8 § 4 de la RIPA et toutes les données de communication associées doivent être traités dans le respect des garanties que le ministre compétent a approuvées conformément à l'obligation que lui impose la RIPA. Ces garanties sont portées à la connaissance du Commissaire à l'interception des communications, et doivent répondre aux exigences de l'article 15 énoncées ci-dessous. Les mandats relevant de l'article 8 § 4 doivent en outre satisfaire aux garanties énoncées à l'article 16. Tout manquement à ces garanties doit être signalé au Commissaire à

l'interception des communications. Les agences interceptrices doivent vérifier régulièrement que leurs garanties internes restent à jour et effectives. Au cours de ces vérifications périodiques, elles doivent rechercher s'il serait sûr et utile de rendre publiques des procédures internes jusque-là confidentielles.

Les garanties posées à l'article 15 de la RIPA

7.2. L'article 15 de la RIPA impose que la divulgation, la copie et la conservation des éléments interceptés soient limitées au minimum nécessaire dans un but autorisé. L'article 15 § 4 dispose qu'une chose est nécessaire dans l'un des buts autorisés si les éléments interceptés :

- restent ou sont susceptibles de devenir nécessaires dans l'un quelconque des buts énoncés à l'article 5 § 3 – c'est-à-dire dans l'intérêt de la sécurité nationale, aux fins de la prévention ou de la détection des infractions graves, ou aux fins, dans des circonstances que le ministre estime relever de l'intérêt de la sécurité nationale, de la sauvegarde de la prospérité économique du Royaume-Uni ;
- sont nécessaires pour faciliter l'exercice des fonctions du ministre compétent relevant du chapitre I de la partie I de la RIPA ;
- sont nécessaires pour faciliter l'exercice de l'une quelconque des fonctions du Commissaire à l'interception des communications ou de l'IPT ;
- sont nécessaires pour qu'une personne chargée de conduire des poursuites pénales dispose des informations dont elle a besoin pour déterminer les mesures à prendre en vue de se conformer à son obligation de garantir l'équité des poursuites ; ou
- sont nécessaires pour l'exécution de toute obligation imposée par la législation relative aux archives publiques.

Diffusion des éléments interceptés

7.3. Le nombre de personnes auxquelles l'un quelconque des éléments interceptés est divulgué et l'ampleur de la divulgation doivent être limités au minimum nécessaire à la réalisation des buts autorisés par l'article 15 § 4 de la RIPA. Cette obligation s'applique aussi bien à la divulgation au sein de l'agence qu'à la divulgation hors de l'agence. Elle se traduit par l'interdiction de divulguer les éléments interceptés à des personnes qui ne disposent pas de l'habilitation adéquate et par le principe du besoin d'en connaître, selon lequel les éléments en question ne peuvent être divulgués qu'aux personnes dont les fonctions se rattachent à l'un des buts autorisés et qui ont besoin d'en avoir connaissance pour accomplir leurs fonctions. De même, le destinataire ne doit recevoir que la partie des éléments interceptés qu'il a besoin de connaître. Dans les cas où un résumé des éléments interceptés suffit, il n'y a pas lieu d'en divulguer davantage.

7.4. Ces obligations s'appliquent non seulement à la personne qui a intercepté les éléments mais aussi à toutes les personnes à qui ils sont ensuite divulgués. Dans certains cas, le respect de ces obligations imposera à la personne à laquelle l'information a été divulguée d'obtenir l'autorisation de celui dont elle émane avant de la partager à son tour. Dans d'autres cas, des garanties expresses sont appliquées aux destinataires secondaires des informations.

7.5. Lorsque des éléments interceptés sont divulgués à des autorités d'un pays ou territoire non britannique, l'agence doit prendre des mesures raisonnables pour s'assurer que ces autorités ont mis en place et appliquent les procédures nécessaires

pour protéger les éléments interceptés et pour garantir qu'ils ne seront divulgués, copiés, distribués et conservés que dans la stricte mesure du nécessaire. En particulier, les éléments interceptés ne doivent pas être divulgués aux autorités d'un autre pays ou territoire sans l'accord exprès de l'agence dont ils émanent, et ils doivent être restitués à celle-ci ou détruits de manière sécurisée lorsqu'ils ne sont plus nécessaires.

Copie

7.6. Les éléments interceptés ne peuvent être copiés que dans la mesure nécessaire à la réalisation des buts autorisés par l'article 15 § 4 de la RIPA. On entend par « copies » non seulement les copies directes de l'intégralité des éléments interceptés, mais aussi les extraits et résumés présentés comme le produit d'une interception, et toute mention d'une interception faisant état de l'identité des destinataires ou expéditeurs des éléments interceptés. Ces restrictions se traduisent par des exigences particulières en matière de traitement des copies, extraits et résumés qui sont faits de ces éléments, c'est-à-dire par l'obligation de conserver la trace de leur réalisation, de leur distribution et de leur destruction.

Stockage

7.7. Les éléments interceptés et la totalité des copies, extraits et résumés qui en sont faits doivent être traités et stockés de manière sécurisée, afin de réduire au minimum le risque de perte ou de vol. Ils doivent être conservés de manière à être inaccessibles aux personnes qui n'ont pas le niveau d'habilitation requis. Cette obligation de conserver le produit d'une interception de manière sécurisée s'applique à tous ceux qui sont responsables de son traitement, y compris les fournisseurs de services de communication. Les implications pratiques de cette obligation pour les fournisseurs de services de communication sont détaillées dans le cadre des discussions qu'ils ont avec le gouvernement avant qu'une instruction prise en application de l'article 12 ne leur soit notifiée (voir le paragraphe 3.13).

Destruction

7.8. Les éléments interceptés, et la totalité des copies, extraits et résumés pouvant être identifiés comme étant les produits d'une interception doivent être marqués pour suppression et détruits de manière sécurisée aussitôt que possible après qu'ils ne sont plus nécessaires à la réalisation d'un but autorisé. Si ces éléments interceptés sont conservés, il faut vérifier régulièrement que la raison justifiant leur conservation demeure valable au regard de l'article 15 § 3 de la RIPA.

7.9. Lorsqu'une agence interceptrice procède à une interception dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA et reçoit des éléments interceptés non analysés et les données de communication associées, elle doit fixer (ou déterminer système par système) une durée maximale de conservation pour les différentes catégories de données, en fonction de leur nature et du degré de l'intrusion dans la vie privée des individus concernés résultant de leur collecte. Les durées ainsi fixées ne doivent normalement pas dépasser deux ans, et elles doivent être convenues avec le Commissaire à l'interception des communications. Les données ne peuvent être conservées au-delà de la durée maximale de conservation qui leur est applicable que sur autorisation préalable délivrée par un haut responsable de l'agence interceptrice au motif que la prolongation de leur conservation a été jugée nécessaire et proportionnée au but visé. Si par la suite on estime que la prolongation de la conservation de ces données ne répond plus aux critères de nécessité et de proportionnalité, celles-ci doivent être supprimées. Dans la mesure du possible, le respect des durées de conservation des données est assuré par un processus de

suppression automatisée qui se déclenche lorsque la durée maximale de conservation applicable aux données en question est atteinte.

Habilitation du personnel

7.10. Toutes les personnes pouvant avoir accès aux éléments interceptés ou besoin de consulter un rapport les concernant doit disposer du niveau d'habilitation adéquat. Chaque année, les responsables doivent rechercher s'il existe des réserves susceptibles de donner lieu au réexamen de l'habilitation de tel ou tel membre du personnel. L'habilitation de chaque membre du personnel doit aussi faire l'objet d'un réexamen périodique. Lorsqu'il est nécessaire qu'un membre d'une agence divulgue des éléments interceptés à un autre membre, il incombe au premier de vérifier que le second dispose de l'habilitation nécessaire.

Les garanties posées à l'article 16 de la RIPA

7.11. L'article 16 de la RIPA prévoit des garanties supplémentaires pour les éléments interceptés dans le cadre d'un mandat émis en vertu de l'article 8 § 4. Il dispose que ces garanties doivent :

- assurer que les éléments interceptés ne soient lus, consultés ou écoutés par quiconque que dans la mesure où ils relèvent d'un certificat ; et
- encadrer l'utilisation de facteurs de sélection concernant les communications d'individus dont on sait qu'ils se trouvent actuellement dans les îles Britanniques.

7.12. De plus, toute sélection d'éléments interceptés doit être proportionnée à la situation dans laquelle elle s'inscrit (compte tenu de l'article 6 § 1 de la loi de 1998 sur les droits de l'homme [*Human Rights Act 1998*]).

7.13. Le certificat garantit qu'un processus de sélection sera appliqué aux éléments interceptés dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA, afin que seuls les éléments qu'il décrit puissent être examinés (c'est-à-dire être lus, consultés ou écoutés) par un être humain. Aucun agent ne peut accéder aux données autrement que dans la limite prévue par le certificat.

7.14. En général, il faut, lorsque c'est techniquement possible, utiliser des systèmes automatisés pour réaliser une sélection conformément à l'article 16 § 1 de la RIPA. À titre exceptionnel, un certificat peut permettre à un nombre limité de membres du personnel spécialement autorisés d'accéder à des éléments interceptés sans que ceux-ci n'aient été traités ou filtrés par un système automatisé. Cet accès ne peut être permis que dans la mesure nécessaire pour déterminer si les éléments en question relèvent des principales catégories permettant de les sélectionner en vertu du certificat, ou pour vérifier que la méthode [de filtrage] utilisée demeure à jour et efficace. Cette vérification doit elle-même revêtir un caractère nécessaire pour les motifs visés à l'article 5 § 3 de la RIPA. Cela fait, toute copie des éléments produite à ces fins doit être détruite conformément à l'article 15 § 3 de la RIPA. Cette vérification par des agents humains doit être circonscrite au strict minimum et doit autant que possible être évitée au profit de techniques de sélection automatisées. La vérification est contrôlée par le Commissaire à l'interception des communications lors de ses inspections.

7.15. Les éléments recueillis dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA ne peuvent être lus, consultés ou écoutés que par des personnes autorisées qui suivent régulièrement une formation obligatoire sur les dispositions de la RIPA, et en particulier sur le fonctionnement de l'article 16 de cette loi et sur les exigences de nécessité et de proportionnalité. Ces exigences et

procédures sont mentionnées dans des directives internes fournies à toutes les personnes autorisées, qui doivent être expressément invitées à examiner les garanties prévues par la loi. Toutes les personnes autorisées doivent avoir le niveau d'habilitation adéquat (voir le paragraphe 7.10 pour plus d'informations).

7.16. Avant qu'une personne autorisée ne puisse lire, consulter ou écouter des éléments, les raisons pour lesquelles l'accès à ces éléments est requis au sens et en vertu de l'article 16 de la RIPA et du certificat applicable, et les raisons pour lesquelles cet accès constitue une mesure proportionnée au but visé doivent être enregistrées. Sauf dans les cas où les éléments ou les systèmes automatisés sont vérifiés de la manière décrite au paragraphe 7.14, l'enregistrement doit indiquer, au moyen de critères précis, les éléments auxquels l'accès est demandé, et les systèmes doivent, dans la mesure du possible, empêcher l'accès à ces éléments tant que l'enregistrement n'a pas été fait. L'enregistrement doit mentionner toutes les circonstances qui sont susceptibles de donner lieu dans une mesure plus ou moins grande à une atteinte collatérale à la vie privée, et toutes les mesures prises pour réduire l'ampleur de cette intrusion collatérale. Tous les enregistrements doivent être conservés pour pouvoir être présentés en cas d'examen ou d'audit ultérieur.

7.17. L'accès aux données décrit au paragraphe 7.15 doit être limité dans le temps, mais il peut être renouvelé. Si l'accès est renouvelé, il faut mettre à jour l'enregistrement correspondant en indiquant la raison du renouvellement. Des systèmes bloquant l'accès aux données à l'expiration de la durée de validité de l'accès en l'absence de demande de renouvellement doivent être mis en place. Lorsque le maintien de l'accès aux données n'est pas souhaité, la raison doit aussi en être indiquée dans l'enregistrement correspondant.

7.18. Des audits doivent être réalisés périodiquement aux fins de la vérification du respect des exigences énoncées à l'article 16 de la RIPA et au chapitre 3 du présent code. Les personnes qui procèdent à ces audits doivent s'assurer de la bonne tenue des enregistrements des demandes d'accès aux données pour lecture, consultation ou écoute et, en particulier, vérifier que les éléments demandés relèvent des questions pour lesquelles le ministre compétent a émis un certificat. Il faut signaler à la hiérarchie toute erreur et tout manquement à la procédure, et prendre en pareil cas des mesures correctives. Toute défaillance grave doit être portée à l'attention de la haute hiérarchie, et tout manquement aux garanties doit être signalé au Commissaire à l'interception des communications (voir le paragraphe 7.1). Tous les rapports de renseignement établis par les personnes autorisées doivent faire l'objet d'un audit de contrôle qualité.

7.19. Lorsqu'un facteur de sélection vise un individu dont on sait qu'il se trouve actuellement dans les îles Britanniques et que le but ou l'un des buts de la mesure envisagée est de découvrir des éléments contenus dans des communications dont cet individu est l'expéditeur ou le destinataire, la demande doit, pour répondre aux exigences de la RIPA exposées au paragraphe 6.3 ci-dessus, être faite au ministre compétent, ou à un haut responsable s'il s'agit d'un cas d'urgence, et elle doit exposer les raisons pour lesquelles une modification du certificat émis en vertu de l'article 8 § 4 à l'égard de cet individu est nécessaire dans un but relevant de l'article 5 § 3 et proportionnée au but visé par l'intervention autorisée en vertu de l'article 8 § 4.

7.20. Le ministre compétent doit veiller à ce que les garanties soient appliquées avant que l'interception réalisée dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA ne puisse commencer. Le Commissaire à l'interception des communications est tenu de vérifier le caractère adéquat des garanties.

(...)

8. DIVULGATION TENDANT À ASSURER L'ÉQUITÉ DU PROCÈS PÉNAL

(...)

Éléments exclus des procédures judiciaires

8.3. En principe, l'existence éventuelle d'une interception et les éléments interceptés eux-mêmes ne jouent aucun rôle dans les procédures judiciaires. Ce principe est posé par l'article 17 de la RIPA, qui interdit, dans les procédures judiciaires, les productions de preuves, les interrogatoires, les déclarations ou les communications d'informations susceptibles de révéler l'existence (ou l'absence) d'un mandat émis en vertu de cette loi (ou de la loi de 1985 sur l'interception de communications [*Interception of Communications Act 1985*]). Il implique que ni l'accusation ni la défense ne peuvent utiliser des éléments interceptés. Il garantit l'« égalité des armes » exigée par l'article 6 de la Convention européenne des droits de l'homme.

(...)

10. SUPERVISION

10.1. La RIPA prévoit la nomination d'un Commissaire à l'interception des communications, chargé de superviser de manière indépendante l'exercice des pouvoirs conférés par le régime d'interception sur mandat découlant du chapitre I de la partie I de ce texte.

10.2. Le Commissaire inspecte deux fois par an chacune des neuf agences interceptrices. Ces inspections ont pour objectif principal de lui permettre de disposer des informations nécessaires à l'exercice des missions que lui attribue l'article 57 de la RIPA et d'établir son rapport en vertu de l'article 58. Elles peuvent comprendre l'inspection ou l'examen :

- des systèmes mis en place pour l'interception des communications ;
- des données pertinentes conservées par l'agence interceptrice ;
- de la licéité des interceptions réalisées ; et
- des éventuelles erreurs et des systèmes destinés à prévenir ces erreurs.

10.3. Toutes les personnes qui exercent des pouvoirs conférés par le chapitre I de la partie I de la RIPA doivent signaler au Commissaire toute action qu'elles pensent être contraire aux dispositions de la RIPA et tout manquement aux garanties posées à l'article 15 de la RIPA. Elles doivent également répondre à toute demande que leur adresse le Commissaire en lui fournissant les informations dont il a besoin pour s'acquitter de sa mission. »

5. La déposition de Charles Farr

97. Dans la déposition qu'il a faite dans le cadre de l'affaire *Liberty*, Charles Farr a déclaré que, à l'exception des indications figurant dans la RIPA, dans le code de 2010 et dans le projet de code de 2016 (qui avait alors été publié pour consultation), les détails complets des procédures visant à assurer le respect des garanties posées aux articles 15 et 16 étaient confidentiels. Il a précisé qu'il avait personnellement examiné ces procédures et qu'il estimait qu'il n'était pas possible de les rendre publiques

en toute sécurité sans nuire à l'efficacité des méthodes d'interception. Il a ajouté que ces procédures avaient toutefois été communiquées au Commissaire à l'interception des communications, qui devait en vertu de la RIPA les contrôler régulièrement. Enfin, il a indiqué que chaque agence interceptrice était tenue d'enregistrer les procédures en question et que tout manquement devait être signalé au Commissaire.

6. Le livre blanc de 2015 « National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom » (Stratégie de sécurité nationale, défense stratégique et sécurité : un Royaume-Uni sûr et prospère)

98. Dans ce livre blanc, le Conseil de sécurité nationale indiquait que ses priorités pour les cinq années à venir consisteraient à :

> « Combattre frontalement le terrorisme sur le territoire national et à l'étranger de manière ferme et globale, et lutter contre l'extrémisme et les idéologies délétères qui le nourrissent. Nous nous maintiendrons au sommet de la hiérarchie mondiale en matière de cybersécurité. Nous nous emploierons à contrer les menaces émanant d'acteurs étatiques. Nous répondrons aux crises avec promptitude et efficacité et nous accroîtrons nos capacités d'adaptation sur le territoire national et à l'étranger.
>
> Contribuer au renforcement de l'ordre international réglementé et de ses institutions, en soutenant les réformes visant à accroître la participation des puissances émergentes. Nous collaborerons avec nos partenaires pour atténuer les conflits et promouvoir la stabilité, la bonne gouvernance et les droits de l'homme.
>
> Accroître notre prospérité en développant nos relations économiques avec les puissances émergentes telles que l'Inde et la Chine, en contribuant à apporter la prospérité partout dans le monde, en investissant dans l'innovation et les compétences, et en soutenant les exportations britanniques dans le domaine de la défense et de la sécurité. »

7. Le jugement rendu par l'IPT le 29 mars 2015 dans l'affaire Belhadj and Others v. Security Service, Secret Intelligence Service, Government Communications Headquarters, the Secretary of State for the Home Department, and the Secretary of State for the Foreign and Commonwealth Office *(IPT/13/132-9/H et IPT/14/86/CH, « l'affaire Belhadj et autres »)*

99. Dans cette affaire, les demandeurs se disaient victimes de violations des articles 6, 8 et 14 de la Convention, alléguant que leurs communications protégées par le secret professionnel des avocats avaient été interceptées. Dans l'affaire *Liberty*, Amnesty International avait allégué que les procédures destinées à protéger les éléments couverts par le secret professionnel des avocats étaient insuffisantes. Ce grief avait été transféré de l'affaire *Liberty* à l'affaire *Belhadj et autres*, et Amnesty International s'était jointe aux autres demandeurs dans cette dernière affaire (paragraphe 52 ci-dessus).

100. Au cours de la procédure, les défendeurs reconnurent que les pratiques qui avaient cours depuis janvier 2010 en matière d'interception/obtention, d'analyse, d'utilisation, de divulgation et de destruction d'éléments couverts par le secret professionnel des avocats n'étaient pas prévues par la loi au sens de l'article 8 § 2 de la Convention et étaient donc illicites car aucune procédure légale n'avait été mise en place pour traiter les éléments en question. Le MI5 et le GCHQ affirmèrent qu'ils s'attacheraient dans les semaines suivantes à réviser leurs règles et procédures à la lumière notamment du projet de code de conduite en matière d'interception de communications.

101. L'IPT tint ensuite une audience à huis clos, avec l'assistance du conseil près le Tribunal (paragraphe 132 ci-dessous), pour déterminer si les défendeurs avaient intercepté ou obtenu des documents ou informations relatifs à des éléments couverts par le secret professionnel des avocats. Le 29 mars 2015, il prononça une décision dans laquelle il concluait que les agences mises en cause ne détenaient que deux documents appartenant à un demandeur et renfermant des éléments couverts par le secret professionnel des avocats, et que ces documents ne contenaient ni ne concernaient aucun conseil juridique. Il considéra donc que le demandeur concerné n'avait subi aucun inconvénient ni aucun dommage, et que sa décision constituait une satisfaction équitable suffisante. Il exigea cependant que le GCHQ s'engage à ce que les parties de ces documents renfermant des éléments protégés par le secret professionnel des avocats soient détruites ou supprimées, qu'une copie des documents soit remise au Commissaire à l'interception des communications pour qu'il les conserve pendant cinq ans, et qu'un rapport confidentiel confirmant la destruction et la suppression des documents soit remis dans un délai de quatorze jours.

102. Par la suite, des projets de modification du code de conduite en matière d'interception de communications et du code de conduite sur l'acquisition et la divulgation de données de communication furent publiés pour consultation, et les codes qui furent adoptés en 2018 à la suite de cette consultation renfermaient des passages étoffés sur l'accès aux informations protégées par le secret ou la confidentialité.

B. L'échange de renseignements

1. L'accord d'échange de renseignements entre le Royaume-Uni et les États-Unis

103. Depuis le 5 mars 1946, un accord sur l'échange de renseignements entre le Royaume-Uni et les États-Unis régit l'échange entre les autorités britanniques et les autorités américaines de renseignements relatifs aux communications « à l'étranger », l'étranger désignant les pays autres que les États-Unis, le Royaume-Uni et les membres du Commonwealth. Dans le

cadre de cet accord, les parties se sont engagées à échanger le produit de certaines opérations d'interception de communications à l'étranger.

2. Le cadre légal applicable aux activités des services de renseignement

104. Il y a trois services de renseignement au Royaume-Uni : le *Security Service* (« MI5 »), le *Secret Intelligence Service* (« MI6 ») et le GCHQ.

a) Activités du MI5

105. En vertu de l'article 2 de la loi de 1989 sur les services de sécurité (*Security Service Act 1989*), le Directeur général du MI5, qui est nommé par le ministre de l'Intérieur, est tenu de veiller à la mise en place de procédures visant à assurer que le MI5 ne recueille aucune autre information que celles nécessaires au bon exercice de ses fonctions et qu'il ne divulgue aucune information sauf dans la mesure nécessaire à cette fin ou aux fins de la prévention et de la détection des infractions graves ou d'une procédure pénale.

106. En vertu de l'article 1 de la loi sur les services de sécurité, le MI5 a pour fonctions d'assurer la protection de la sécurité nationale et, en particulier, la protection contre les menaces provenant de l'espionnage, du terrorisme et du sabotage, des activités d'agents de puissances étrangères et des actions visant à saper ou à renverser la démocratie parlementaire par des moyens politiques, par des actions collectives ou par la violence ; de protéger la prospérité économique du Royaume-Uni contre les menaces provenant des actions ou intentions de personnes situées hors des îles Britanniques ; et d'appuyer les activités de prévention et de détection des infractions graves menées par les forces de police, le service de lutte contre la criminalité et les autres services des forces de l'ordre.

b) Activités du MI6

107. L'article 2 de la loi de 1994 sur les services de renseignement (*Intelligence Services Act 1994*) dispose que le Chef du MI6, qui est nommé par le ministre des Affaires étrangères et du Commonwealth (tel était alors son titre), est tenu de veiller à la mise en place de procédures visant à assurer que le MI6 ne recueille aucune autre information que celles nécessaires au bon exercice de ses fonctions et qu'il ne divulgue aucune information sauf dans la mesure nécessaire à cette fin, dans l'intérêt de la sécurité nationale, ou aux fins de la prévention et de la détection des infractions graves ou d'une procédure pénale.

108. En vertu de l'article 1 de la loi sur les services de renseignement, le MI6 a pour fonctions d'obtenir et de fournir des informations relatives aux actions et intentions de personnes situées hors des îles Britanniques, et d'accomplir d'autres tâches relatives à ces actions et intentions. Ces

fonctions ne peuvent être exercées que dans l'intérêt de la sécurité nationale, en particulier pour la défense de l'État et l'application de sa politique étrangère ; dans l'intérêt de la prospérité économique du Royaume-Uni ; ou à l'appui de la prévention et de la détection des infractions graves.

c) Activités du GCHQ

109. L'article 4 de la loi sur les services de renseignement dispose que le Directeur du GCHQ, qui est nommé par le ministre des Affaires étrangères et du Commonwealth (tel était alors son titre), est tenu de veiller à la mise en place de procédures visant à assurer que le GCHQ ne recueille aucune autre information que celles nécessaires au bon exercice de ses fonctions et qu'il ne divulgue aucune information, sauf dans la mesure nécessaire.

110. En vertu de l'article 3 de la loi sur les services de renseignement, l'une des fonctions du GCHQ est de surveiller les émissions électromagnétiques, acoustiques et autres ainsi que les équipements qui les produisent et de s'y introduire, et d'obtenir et fournir des informations provenant de ces émissions ou équipements, liées à ceux-ci ou provenant d'éléments cryptés. Cette fonction ne peut être exercée que dans l'intérêt de la sécurité nationale, en particulier pour la défense de l'État et l'application de sa politique étrangère ; dans l'intérêt de la prospérité économique du Royaume-Uni en ce qui concerne les actions et intentions de personnes se trouvant hors des îles Britanniques ; ou à l'appui de la prévention et de la détection des infractions graves.

d) La loi de 2008 sur la lutte contre le terrorisme (Counter-Terrorism Act 2008, « la loi sur la lutte contre le terrorisme »)

111. L'article 19 de la loi sur la lutte contre le terrorisme permet la divulgation d'informations à n'importe lequel des services de renseignement aux fins de l'exercice de ses fonctions. Les informations obtenues par un service de renseignement dans le cadre de l'exercice de certaines de ses fonctions peuvent être utilisées par ce service dans le cadre de l'exercice de ses autres fonctions.

112. Lorsque le MI5 a obtenu des informations, il peut les divulguer aux fins du bon exercice de ses fonctions, aux fins de la prévention ou de la détection des infractions graves, ou aux fins de toute procédure pénale. Lorsque le MI6 a obtenu des informations, il peut les divulguer aux fins du bon exercice de ses fonctions, dans l'intérêt de la sécurité nationale, aux fins de la prévention ou de la détection des infractions graves, ou aux fins de toute procédure pénale. Lorsque le GCHQ a obtenu des informations, il peut les divulguer aux fins du bon exercice de ses fonctions ou aux fins de toute procédure pénale.

e) La loi de 1998 sur la protection des données (Data Protection Act 1998, « la loi sur la protection des données »)

113. La loi sur la protection des données est le texte qui transpose en droit interne la directive 95/46/CE sur la protection des données à caractère personnel. Chaque service de renseignement est « responsable du traitement des données » aux fins de la loi sur la protection des données et, en cette qualité, est tenu de respecter – sauf dérogation prenant la forme d'un certificat ministériel – les principes de protection des données énoncées dans la partie I de l'annexe 1 à cette loi, et notamment les suivants :

> « 5) Les données personnelles faisant l'objet d'un traitement, quelles qu'en soient la ou les fins, ne sont pas conservées plus longtemps que nécessaire à cette ou ces fins (...)

et

> « 7) Des mesures techniques et organisationnelles appropriées sont prises contre le traitement non autorisé ou illicite de données personnelles et contre la perte, la destruction et l'endommagement accidentels des données personnelles. »

f) La loi de 1989 sur les secrets officiels (Official Secrets Act 1989, « la loi sur les secrets officiels »)

114. Un membre des services de renseignement commet une infraction à l'article 1 § 1 de la loi sur les secrets officiels s'il divulgue, sans y avoir été dûment habilité, une information, un document ou un autre élément relatifs à la sécurité ou au renseignement dont il est en possession du fait de sa qualité de membre de ces services.

g) La loi de 1998 sur les droits de l'homme (Human Rights Act 1998, « la loi sur les droits de l'homme »)

115. L'article 6 de la loi sur les droits de l'homme dispose qu'il est illégal, pour une autorité publique, d'agir de manière incompatible avec un droit garanti par la Convention.

3. Le code de conduite en matière d'interception de communications

116. Après l'affaire *Liberty*, les informations figurant dans la note de divulgation du 9 octobre (paragraphes 33 et 36 ci-dessus) ont été incorporées dans le code de conduite en matière d'interception de communications. Les passages pertinents de ce code sont ainsi libellés :

> « 12. RÈGLES APPLICABLES AUX DEMANDES ADRESSÉES À UN GOUVERNEMENT ÉTRANGER ET AU TRAITEMENT DE COMMUNICATIONS INTERCEPTÉES NON ANALYSÉES
>
> **Champ d'application du présent chapitre**
>
> 12.1. Le présent chapitre s'applique aux agences interceptrices qui réalisent des interceptions dans le cadre de mandats émis en vertu de l'article 8 § 4 de la RIPA.

Demandes d'assistance ne relevant pas d'un accord d'entraide internationale

12.2. Une agence interceptrice ne peut adresser au gouvernement d'un pays ou territoire non britannique une demande aux fins de l'obtention de communications interceptées non analysées (et des données de communication associées) hors du cadre d'un accord d'entraide internationale que dans l'un des deux cas suivants :

- le ministre compétent a déjà émis un mandat d'interception à cet égard en vertu de la RIPA, l'assistance du gouvernement étranger est nécessaire pour obtenir les communications en question car elles ne peuvent pas être obtenues dans le cadre du mandat d'interception émis en vertu de la RIPA, et il est nécessaire et proportionné au but visé que l'agence interceptrice les obtienne ; ou
- le fait de demander ces communications en l'absence de mandat d'interception émis à cet égard en vertu de la RIPA ne constitue pas un contournement délibéré de la RIPA et ne fait pas échec d'une autre manière aux objectifs de la RIPA (par exemple, il n'est pas faisable techniquement d'obtenir ces communications au moyen d'une interception réalisée en vertu de la RIPA), et il est nécessaire et proportionné au but visé que l'agence interceptrice les obtienne.

12.3. Une demande relevant du second cas visé au paragraphe 12.2 ne peut être faite que dans des circonstances exceptionnelles et doit faire l'objet d'un examen et d'une décision du ministre compétent lui-même.

12.4. Aux fins des paragraphes ci-dessus, un « mandat d'interception émis à cet égard en vertu de la RIPA » désigne : i) un mandat émis en vertu de l'article 8 § 1 à l'égard du sujet concerné ; ii) un mandat émis en vertu de l'article 8 § 4 accompagné, d'une part, d'un certificat qui comprend une ou plusieurs « descriptions des éléments à intercepter » (au sens de l'article 8 § 4 b)) couvrant les communications du sujet et, d'autre part, d'un document modificatif approprié établi conformément à l'article 16 § 3 (pour les individus dont on sait qu'ils se trouvent dans les îles Britanniques) ; ou iii) un mandat émis en vertu de l'article 8 § 4 et accompagné d'un certificat qui comprend une ou plusieurs « descriptions des éléments à intercepter » couvrant les communications du sujet (pour les autres individus).

Garanties applicables au traitement des communications interceptées non analysées fournies par un gouvernement étranger

12.5. Si une demande relevant du second cas visé au paragraphe 12.2 est approuvée par le ministre sans être liée à des sélecteurs spécifiques, l'agence interceptrice ne peut examiner selon l'un quelconque des facteurs visés à l'article 16 § 2 a) et b) de la RIPA aucune des communications obtenues, à moins que le ministre n'ait personnellement examiné et approuvé le projet d'examen de ces communications en fonction de ces facteurs[1].

12.6. Lorsque les agences interceptrices obtiennent des communications interceptées ou des données de communication de la manière visée au paragraphe 12.2

[1] Toutes les autres demandes relevant du paragraphe 12.2 (qu'elles s'accompagnent ou non d'un mandat d'interception délivré en vertu de la RIPA) visent à l'obtention de communications à destination ou en provenance de sélecteurs spécifiques (c'est-à-dire liées à un ou plusieurs individus spécifiques), ou en rapport avec de tels sélecteurs. En pareil cas, le ministre compétent aura déjà approuvé la demande liée à un ou plusieurs individus spécifiques, comme le prévoient les paragraphes [sic.] 12.2.

ou qu'elles les reçoivent du gouvernement d'un pays ou territoire non britannique dans des circonstances où ces communications et données se présentent comme le produit d'une interception (sauf dans le cadre d'un accord d'entraide internationale), le contenu des communications et les données de communication ainsi obtenus ou reçus doivent être soumis aux mêmes règles et garanties internes que celles qui s'appliquent aux contenus et données de même catégorie obtenus directement par les agences interceptrices dans le cadre d'une interception réalisée en vertu de la RIPA.

12.7. Toutes les demandes faites au gouvernement d'un pays ou territoire non britannique aux fins de l'obtention de communications interceptées non analysées (et des données de communication associées) en l'absence de mandat d'interception émis à cet égard en vertu de la RIPA sont notifiées au Commissaire à l'interception des communications. »

C. L'acquisition de données de communication

117. Le chapitre II de la partie I de la RIPA posait le cadre dans lequel les autorités publiques pouvaient obtenir des données de communication auprès des fournisseurs de services de communication.

118. En vertu de l'article 22, l'autorisation d'acquérir des données de communication auprès d'un fournisseur de services de communication était accordée par une « personne désignée », qui devait occuper au sein des autorités publiques compétentes une fonction, un rang ou une position fixés par une ordonnance du ministre compétent. La personne désignée pouvait soit autoriser des personnes relevant de la même « autorité publique compétente » qu'elle à « réaliser l'intervention à laquelle s'appliqu[ait] le (...) chapitre [II] » (autorisation relevant de l'article 22 § 3) soit, par un avis adressé au fournisseur de services de communication, ordonner à celui-ci de lui communiquer des données déjà en sa possession, ou d'obtenir des données afin de les lui communiquer (avis relevant de l'article 22 § 4). Aux fins de l'article 22 § 3, les « autorités publiques compétentes » comprenaient la police, le service de lutte contre la criminalité, le service des recettes et douanes, tous les services de renseignement, et toute autorité publique déclarée compétente par une ordonnance du ministre compétent.

119. L'article 22 § 2 disposait également que la personne désignée ne pouvait accorder une autorisation relevant de l'article 22 § 3 ou adresser un avis relevant de l'article 22 § 4 que si elle l'estimait nécessaire pour l'un des motifs suivants :

« a) dans l'intérêt de la sécurité nationale ;

b) aux fins de la prévention ou de la détection des infractions ou du maintien de l'ordre ;

c) dans l'intérêt de la prospérité économique du Royaume-Uni ;

d) dans l'intérêt de la sécurité publique ;

e) aux fins de la protection de la santé publique ;

f) aux fins du calcul ou du recouvrement de tout impôt, droit, redevance ou autre taxe, contribution ou charge dus à l'administration ;

g) en cas d'urgence, aux fins d'empêcher un décès, une blessure ou une atteinte à la santé physique ou mentale d'une personne, ou de limiter la gravité d'une blessure ou d'une atteinte à la santé physique ou mentale d'une personne ; ou

h) à toute fin (ne relevant pas des alinéas a) à g)) énoncée en vertu du présent alinéa dans une ordonnance prise par le ministre compétent. »

120. Pour émettre une autorisation ou un avis en vertu de l'article 22, la personne désignée devait aussi estimer que l'obtention des données était une mesure proportionnée au but visé.

121. Le chapitre II de la RIPA était complété par le code de conduite sur l'acquisition et la divulgation de données de communication (*Acquisition and Disclosure of Communications Data: Code of practice*) établi en vertu de l'article 71 de la RIPA.

D. La pratique et la procédure de l'IPT

1. La RIPA

122. L'IPT a été instauré par l'article 65 § 1 de la RIPA pour examiner les allégations de citoyens s'estimant victimes, de la part des autorités, d'une ingérence illicite dans leurs communications à l'occasion des activités relevant de cette loi. L'IPT est compétent pour examiner tout grief d'une personne alléguant que ses communications ont été interceptées et, si tel est le cas, pour examiner la base de cette interception.

123. Les nominations des membres de l'IPT sont par nature essentiellement judiciaires, mais elles diffèrent selon que les candidats proposés sont des juges en fonction des juridictions supérieures d'Angleterre et du pays de Galles, d'Écosse ou d'Irlande du Nord (les « membres judiciaires ») ou des « membres non judiciaires » recrutés parmi des juristes chevronnés ayant au moins dix ans d'expérience et n'exerçant pas à plein temps les fonctions de juge. Le processus de recrutement des membres judiciaires de l'IPT au sein de la magistrature d'Angleterre et du pays de Galles est conduit par le *Judicial Office*, au nom du *Lord Chief Justice*. Les juges de la *High Court* d'Angleterre et du pays de Galles sont invités par le *Judicial Office* à manifester leur intérêt pour une nomination à l'IPT. Ensuite, les candidats s'entretiennent avec un comité composé du président de l'IPT, d'un membre non judiciaire de l'IPT et d'un commissaire qui n'est ni juriste ni magistrat et qui appartient à la commission de nomination des juges (*Judicial Appointments Commission*). À l'issue des entretiens, le comité fait un compte rendu au *Lord Chief Justice*, qui adresse par écrit au ministre de l'Intérieur des recommandations officielles de nomination. Il incombe ensuite à ce dernier de demander par écrit au Premier ministre l'autorisation de solliciter auprès de Sa Majesté la

Reine des lettres patentes pour les nominations recommandées. Le Premier ministre recommande les candidats retenus à Sa Majesté la Reine, qui officialise les nominations par lettres patentes. Pour leur part, les membres non judicaires de l'IPT sont recrutés par concours. À cet effet, l'IPT publie dans un certain nombre de quotidiens nationaux et sur des sites de recrutement des annonces pour le recrutement de membres non judiciaires, invitant les personnes possédant les qualifications voulues à manifester leur intérêt. Le processus de recrutement des membres non judiciaires est en tous points identique à celui des membres judiciaires, sauf qu'il ne fait pas intervenir le *Lord Chief Justice*. Dans sa composition actuelle, l'IPT comprend cinq membres judiciaires (deux membres de la *Court of Appeal* d'Angleterre (dont l'un est président de l'IPT), un membre de la *High Court* d'Angleterre et deux membres de l'*Outer House* de la *Court of Session* d'Écosse (dont l'un est vice-président de l'IPT)) et cinq membres non judiciaires (dont l'un est un juge retraité de la *High Court* d'Irlande du Nord).

124. En vertu de l'article 67 §§ 2 et 3 c), l'IPT doit appliquer les mêmes principes que les tribunaux statuant dans le cadre d'une demande de contrôle juridictionnel. Il n'a toutefois pas le pouvoir de prononcer une déclaration d'incompatibilité s'il juge la législation primaire incompatible avec la Convention européenne des droits de l'homme car il n'est pas une juridiction (*court*) au sens de l'article 4 de la loi sur les droits de l'homme.

125. En vertu de l'article 68 §§ 6 et 7, les personnes ayant pris part à l'autorisation ou à l'exécution d'un mandat d'interception sont tenues de se conformer à toute demande de divulgation ou de communication de documents ou d'informations faite par l'IPT.

126. En vertu de l'article 68 § 4, l'IPT peut octroyer une indemnité et ordonner toute autre mesure qu'il juge appropriée lorsqu'il statue en faveur du plaignant. Il peut ainsi prononcer l'annulation rétroactive ou non d'un mandat et ordonner la destruction de tous les éléments obtenus dans le cadre de ce mandat (article 67 § 7). Lorsqu'il fait droit à une plainte déposée devant lui, il doit en principe en aviser le Premier ministre (article 68 § 5).

127. L'article 68 § 1 donne compétence à l'IPT pour fixer son règlement de procédure, toutefois l'article 69 § 1 dispose que le ministre compétent peut aussi énoncer des règles de procédure.

2. Le règlement de 2000 du Tribunal des pouvoirs d'enquête (Investigatory Powers Tribunal Rules 2000, « le règlement »)

128. Ce règlement a été adopté par le ministre compétent afin d'encadrer différents aspects de la procédure menée devant l'IPT.

129. L'article 9, tel qu'en vigueur à l'époque pertinente, autorisait l'IPT à tenir, à tout stade de son examen de l'affaire, des audiences dans le cadre desquelles le plaignant pouvait formuler des observations, déposer et faire comparaître des témoins. Ce texte disposait également que les procédures de

l'IPT, y compris les éventuelles audiences, devaient se tenir à huis clos. Toutefois, dans les affaires IPT/01/62 et IPT/01/77, l'IPT a décidé de son propre chef qu'il lui était loisible d'opter pour la tenue d'une audience publique, sous réserve du respect de l'obligation générale que lui imposait l'article 6 § 1 d'empêcher la divulgation d'informations sensibles. Depuis qu'il s'est engagé à tenir des audiences publiques dans la mesure du possible, l'IPT publie ses décisions importantes sur son site internet sous réserve que celles-ci ne comportent aucun risque de divulgation d'informations préjudiciables.

130. En vertu de l'article 11 du règlement, l'IPT pouvait recevoir n'importe quel type de preuve, même des preuves non recevables devant un tribunal.

131. En vertu de l'article 6 du règlement, l'IPT devait veiller, dans l'exercice de ses fonctions, à ce qu'il ne soit fait aucune divulgation d'informations contraire à l'intérêt public ou préjudiciable à la sécurité nationale, à la prévention ou à la détection des infractions graves, à la prospérité économique du Royaume-Uni ou à l'accomplissement des missions de l'un quelconque des services de renseignement.

3. Le Conseil près le Tribunal

132. L'IPT peut désigner un Conseil près le Tribunal chargé de présenter des observations au nom des plaignants lors des audiences auxquelles ceux-ci ne peuvent être représentés. Dans l'affaire *Liberty*, le Conseil près le Tribunal a décrit son rôle de la manière suivante :

> « Le Conseil près le Tribunal joue un rôle différent [de celui des avocats spéciaux qui participent aux procédures à huis clos menées devant certains tribunaux spéciaux], qui s'apparente à celui d'*amicus curiae*. Il a pour fonction d'assister le Tribunal en répondant à toutes ses demandes. Il arrive (par exemple relativement à des questions sur lesquelles toutes les parties sont représentées) que le Tribunal ne précise pas de quel point de vue les observations doivent être faites. En pareil cas, le Conseil présente des observations qui correspondent à sa propre analyse des points de fait et de droit en cause, en s'efforçant de mettre l'accent plus particulièrement sur des points que les parties n'ont pas pleinement développés. Il arrive aussi (en particulier lorsqu'un ou plusieurs intérêts ne sont pas représentés) que le Tribunal invite le Conseil à lui présenter des observations d'un point de vue particulier (normalement du point de vue de la ou des parties dont les intérêts ne sont pas représentés). »

133. Cette description a été admise et validée par l'IPT.

4. R (on the application of Privacy International) v Investigatory Powers Tribunal and others *[2019] UKSC 22*

134. Dans cet arrêt, rendu le 15 mai 2019, la Cour suprême a jugé que l'article 67 § 8 de la RIPA n'excluait pas le contrôle juridictionnel des décisions de l'IPT.

E. La supervision

135. La partie IV de la RIPA prévoyait à l'origine la désignation par le Premier ministre d'un Commissaire à l'interception des communications (*Interception of Communications Commissioner*) et d'un Commissaire aux services de renseignement (*Intelligence Services Commissioner*), chargés de superviser les activités des services de renseignement.

136. Le Commissaire à l'interception des communications avait pour rôle de contrôler l'interception des communications ainsi que l'acquisition et la divulgation des données de communication par les services de renseignement, les forces de police et les autres autorités publiques. Dans l'exercice de cette mission de contrôle des pratiques suivies en matière de surveillance, le Commissaire à l'interception des communications et ses inspecteurs avaient accès à tous les documents pertinents, y compris les éléments confidentiels, et toutes les personnes participant à des activités d'interception étaient tenues de leur divulguer tous les éléments qu'ils demandaient. L'obligation pour les agences interceptrices de tenir des dossiers garantissait l'accès effectif du Commissaire aux détails des activités de surveillance entreprises. À l'issue de chaque inspection, un rapport contenant des recommandations officielles était adressé au chef de l'autorité publique concernée, laquelle était tenue de confirmer dans un délai de deux mois que ces recommandations avaient été mises en œuvre ou de rendre compte des progrès accomplis. Le Commissaire rendait compte deux fois par an au Premier ministre de l'accomplissement de sa mission et préparait un rapport annuel qui était rendu public (à l'exception des annexes confidentielles) et remis au Parlement.

137. Le Commissaire aux services de renseignement assurait pour sa part une supervision externe indépendante qui portait sur l'utilisation des pouvoirs intrusifs des services de renseignement et de certains services du ministère de la Défense. Il rendait également au Premier ministre des rapports annuels qui étaient remis au Parlement.

138. La loi de 2016 sur les pouvoirs d'enquête (paragraphes 183-190 ci-dessous) a aboli ces dispositions pour autant qu'elles étaient applicables en Angleterre, en Écosse et au pays de Galles. Depuis septembre 2017, c'est le Commissariat aux pouvoirs d'enquête (*Investigatory Powers Commissioner's Office*) qui supervise l'exercice des pouvoirs d'enquête. Ce commissariat est composé d'une quinzaine de commissaires judiciaires, qui sont des juges en exercice ou récemment retraités de la *High Court*, de la *Court of Appeal* ou de la Cour suprême ; d'un panel consultatif technique composé d'experts scientifiques ; et d'une cinquantaine d'agents (inspecteurs, juristes, experts en communications).

F. Le contrôle des opérations d'interception réalisées par les services de renseignement

1. *La déclaration faite en juillet 2013 par la commission parlementaire sur le renseignement et la sécurité relativement aux allégations d'interception de communications par le GCHQ dans le cadre du programme américain PRISM*

139. La commission parlementaire sur le renseignement et la sécurité (« la commission parlementaire ») a été instaurée par la loi de 1994 sur les services de renseignement afin d'examiner les règles, l'administration et les dépenses du MI5, du MI6 et du GCHQ. La loi de 2013 sur la justice et la sécurité (*Justice and Security Act 2013*) lui a attribué expressément la qualité de commission parlementaire, l'a dotée de pouvoirs plus vastes, et a étendu son champ de compétence notamment à la supervision des activités opérationnelles et des activités plus larges de renseignement et de sécurité du gouvernement. En vertu des articles 1 à 4 de la loi de 2013, la commission comprend neuf membres issus des deux chambres du Parlement et, dans l'exercice de leurs fonctions, ces membres ont couramment accès à des éléments classifiés d'un niveau de confidentialité élevé.

140. Après les révélations d'Edward Snowden, la commission parlementaire a enquêté sur l'accès du GCHQ au contenu de communications interceptées dans le cadre du programme américain PRISM, sur le cadre juridique régissant cet accès et sur les procédures que le GCHQ avait mises en place avec son homologue étranger pour le partage d'informations. Dans le cadre de cette enquête, elle a recueilli des informations détaillées auprès du GCHQ et discuté du programme avec la NSA.

141. Elle a conclu que les allégations selon lesquelles le GCHQ avait contourné les lois du Royaume-Uni en utilisant le programme PRISM pour accéder au contenu de communications privées étaient infondées, le GCHQ ayant respecté les obligations légales que lui imposait la loi sur les services de renseignement. Elle a conclu également que dans chacun des cas où le GCHQ avait demandé des informations aux États-Unis, un mandat d'interception signé par un ministre était déjà en place.

2. *Le rapport « Privacy and security: a modern and transparent legal framework » (Vie privée et sécurité : un cadre juridique moderne et transparent)*

142. Après sa déclaration de juillet 2013, la commission parlementaire a mené des investigations plus approfondies sur l'ensemble des capacités des services de renseignement. À l'issue de ces investigations, elle a publié, le 12 mars 2015, un rapport renfermant un volume sans précédent

d'informations relatives aux capacités d'intrusion des services de renseignement.

143. Dans ce rapport, la commission parlementaire estimait que les services de renseignement et de sécurité du Royaume-Uni n'essayaient pas de contourner leurs obligations légales, notamment les exigences posées par la loi sur les droits de l'homme, à laquelle étaient soumises toutes leurs activités. Elle considérait toutefois que, s'étant développé de manière fragmentaire, le cadre juridique était inutilement compliqué. Elle exprimait de fortes préoccupations quant au manque de transparence qui en découlait, qu'elle jugeait contraire à l'intérêt public. Sa recommandation principale était donc de remplacer le cadre juridique en vigueur par une nouvelle loi qui énoncerait clairement les pouvoirs d'intrusion conférés aux services de renseignement, les buts dans lesquels ils pouvaient les exercer et les autorisations requises au préalable.

144. S'agissant de la capacité d'interception en masse du GCHQ, la commission parlementaire indiquait que ses investigations avaient montré que les services de renseignement n'avaient ni le mandat, ni les ressources, ni la capacité technique, ni le souhait d'intercepter toutes les communications des citoyens britanniques ou toutes les communications Internet dans leur ensemble, et que le GCHQ ne lisait donc pas les courriers électroniques de chaque individu se trouvant au Royaume Uni. Au contraire, les systèmes d'interception en masse du GCHQ n'étaient appliqués qu'à une très faible proportion des canaux de transmission qui constituaient le réseau Internet, et la commission estimait établi que le GCHQ appliquait des niveaux de filtrage et de sélection tels que seule une partie des éléments transitant par ces canaux de transmission était collectée. Elle notait également que le filtrage était suivi de recherches ciblées qui garantissaient que seuls les éléments dont on pensait qu'ils présentaient le plus grand intérêt pour le renseignement étaient finalement transmis à un analyste pour examen, de sorte que seule une part minime des éléments collectés était finalement consultée par un être humain.

145. Pour ce qui était des communications Internet, la commission parlementaire considérait que la manière dont étaient distinguées les communications « intérieures » des communications « extérieures » était déroutante et manquait de transparence. Elle suggérait donc que le gouvernement publie une explication permettant de comprendre quelles communications Internet relevaient de quelle catégorie. Elle notait néanmoins que les investigations avaient établi que l'interception en masse ne pouvait pas être utilisée pour cibler les communications d'un individu se trouvant au Royaume-Uni en l'absence d'autorisation spécifique nommant l'intéressé et signée par un ministre.

146. Elle constatait par ailleurs que les mandats émis en vertu de l'article 8 § 4 de la RIPA étaient en eux-mêmes très brefs et que, lorsque le certificat accompagnant le mandat énonçait les catégories de

communications susceptibles d'être examinées, ces catégories étaient exprimées en termes très généraux (par exemple, « des éléments fournissant des renseignements sur le terrorisme (conformément à la définition figurant dans la loi de 2000 sur le terrorisme (version modifiée)), notamment et sans que cette liste soit exhaustive sur des organisations terroristes, des terroristes, des sympathisants actifs, la préparation d'attentats et la collecte de fonds »). Eu égard au caractère très générique de ce type de certificat, la commission parlementaire se demandait s'il était nécessaire qu'il reste secret ou s'il pouvait être publié, par souci de transparence.

147. Même si le certificat émis en vertu de l'article 8 § 4 de la RIPA précisait les catégories générales d'informations susceptibles d'être examinées, la commission parlementaire observait qu'en pratique, c'étaient la sélection des canaux de transmission, l'application de sélecteurs simples et de critères de recherches qui déterminaient quelles communications étaient examinées. Elle aurait donc souhaité avoir l'assurance que ces méthodes étaient soumises au contrôle et à la vérification des ministres et/ou des Commissaires ; or les éléments dont elle disposait indiquaient que ni les ministres ni les Commissaires n'avaient de visibilité significative sur ces questions. Elle recommandait donc que la loi charge le Commissaire à l'interception des communications de vérifier les différents critères de sélection utilisés dans le cadre des interceptions en masse afin de s'assurer qu'ils correspondent directement au certificat et à des exigences de sécurité nationale valables.

148. La commission parlementaire notait que les données de communication étaient capitales pour la plupart des enquêtes menées par les services de renseignement : on pouvait les analyser pour dégager des schémas reflétant certains comportements en ligne particuliers associés à des activités telles que la préparation d'attentats, pour établir des liens, pour se concentrer sur les individus susceptibles de représenter une menace, pour faire en sorte que les interceptions soient correctement ciblées et pour repérer les réseaux et les associations relativement rapidement. Ces données étaient particulièrement utiles aux premiers stades d'une enquête, où les services de renseignement devaient pouvoir déterminer si les personnes associées à une cible étaient liées au projet criminel objet de l'enquête (et devaient donc faire l'objet d'une enquête plus approfondie) ou s'il s'agissait de personnes sans lien avec ce projet. Selon le ministre de l'Intérieur, ces données avaient « joué un rôle important dans toutes les opérations de contre-terrorisme du [MI5] au cours des dix dernières années ». Néanmoins, la commission parlementaire exprimait une inquiétude au sujet de la définition des « données de communication » : si elle admettait qu'il y avait une catégorie de données de communication dont l'interception était moins intrusive que l'interception de contenus, et qui n'appelait donc pas le même niveau de protection, elle considérait qu'il existait aussi certaines catégories de données de communication susceptibles de révéler des détails plus

intimes de la vie privée d'une personne et, dès lors, appelant des garanties plus importantes.

149. Enfin, la commission parlementaire déclarait expressément qu'il était important que les décisions de l'IPT puissent faire l'objet d'un recours au niveau national.

3. Le rapport « A Question of Trust » (Une question de confiance) établi par le contrôleur indépendant de la législation sur le terrorisme à l'issue du contrôle des pouvoirs d'enquête (« le rapport Anderson »)

150. Le contrôleur indépendant de la législation sur le terrorisme est une personne totalement indépendante du gouvernement, nommée par le ministre de l'Intérieur et par le Trésor pour un mandat de trois ans renouvelable. Il est chargé de rendre compte au ministre de l'Intérieur et au Parlement de la mise en œuvre de la législation relative à la lutte contre le terrorisme au Royaume-Uni. Ses rapports sont remis au Parlement, pour éclairer le débat public et politique.

151. L'objet du rapport Anderson, qui a été publié en juin 2015 et qui porte le nom du contrôleur indépendant de l'époque, David Anderson, Q.C., était d'éclairer le débat public et politique sur les menaces auxquelles était exposé le Royaume-Uni, les capacités nécessaires pour y faire face, les garanties mises en place pour la protection de la vie privée, les défis liés à l'évolution de la technologie, les questions relatives à la transparence et à la supervision, et la nécessité éventuelle de modifier la loi ou d'adopter un nouveau texte. Aux fins de l'établissement de ce rapport, le contrôleur indépendant avait disposé d'un accès sans restriction, au plus haut niveau d'habilitation, aux autorités publiques et services gouvernementaux concernés. Il avait également échangé avec des fournisseurs de services, des experts techniques indépendants, des ONG, des universitaires, des juristes, des juges et des autorités de régulation.

152. Dans son rapport, le contrôleur indépendant notait que le cadre légal régissant les pouvoirs d'enquête s'était « développé de manière fragmentaire » et qu'en conséquence, « peu [de lois étaient] plus impénétrables que la RIPA et les textes en découlant ».

153. S'agissant de l'importance des données de communication, il observait qu'elles permettaient aux services de renseignement de se faire une idée des activités de la personne concernée et qu'elles jouaient un rôle décisif dans l'acquisition d'informations relatives à des activités criminelles ou terroristes. Il notait qu'elles permettaient d'identifier les cibles de futures opérations et qu'elles contribuaient aussi à établir que quelqu'un était complètement innocent. Il concluait que la capacité d'utiliser les données de communication (sous réserve des principes de nécessité et de proportionnalité) était d'une importance capitale :

a) pour établir un lien entre un individu et un compte ou une activité (telle que la visite d'un site web ou l'envoi d'un courrier électronique) grâce à la résolution de son adresse IP ;
b) pour déterminer le lieu où se trouvait une personne, généralement grâce au bornage de son téléphone ou aux données GPRS ;
c) pour déterminer comment les suspects ou les victimes communiquaient (par quelles applications ou services) ;
d) pour observer la criminalité en ligne (par exemple, déterminer quels sites web étaient visités à des fins de terrorisme, d'exploitation sexuelle des enfants ou d'acquisition d'armes à feu ou de drogues illicites) ; et
e) pour exploiter les données (par exemple, pour déterminer où, quand et avec qui ou quoi quelqu'un communiquait, comment des logiciels malveillants (*malware*) ou des attaques par déni de service (*denial of service attack*) étaient mis en œuvre, ou encore pour corroborer d'autres éléments de preuve).

154. Il notait également que l'analyse des données de communication pouvait être réalisée rapidement, ce qui la rendait extrêmement utile pour des opérations où la situation évoluait vite, et que l'utilisation de ces données pouvait fournir les éléments nécessaires pour justifier une mesure plus intrusive ou pour rendre d'autres mesures inutiles.

155. Les réformes proposées par le contrôleur indépendant peuvent se résumer ainsi :

a) élaborer une nouvelle loi complète et compréhensible qui remplacerait « les multiples mandats existants » et encadrerait par des limites et des garanties claires tout pouvoir d'intrusion que les autorités publiques pourraient devoir exercer ;
b) revoir et clarifier la définition des « données de contenu » et celle des « données de communication » ;
c) maintenir la possibilité pour les services de sécurité et de renseignement d'intercepter en masse des éléments et les données de communication associées, mais en l'encadrant par des garanties supplémentaires strictes, notamment en soumettant tous les mandats à l'autorisation d'un commissaire judiciaire, membre d'une commission indépendante de la surveillance et du renseignement (« la commission surveillance et renseignement ») à créer ;
d) énoncer dans le certificat accompagnant le mandat les buts pour lesquels des éléments ou des données pourraient être recherchés par référence à des opérations ou des objectifs de

mission précis (par exemple, « projet d'attentat de l'EIIL contre les intérêts britanniques en Irak/en Syrie ») ;

e) créer une nouvelle forme de mandat d'interception en masse limité à l'acquisition de données de communication pour les cas où cette mesure constituerait une solution proportionnée au but visé ;

f) confier le pouvoir de supervision à la future commission de la surveillance et du renseignement et la rendre transparente et accessible au public et aux médias ; et

g) donner à l'IPT le pouvoir de prononcer des déclarations d'incompatibilité et rendre ses décisions susceptibles de recours sur des points de droit.

4. Le rapport « A Democratic Licence to Operate » (Un permis d'intervention démocratique), établi à l'issue du contrôle indépendant des activités de surveillance (« le contrôle de la surveillance »)

156. À la demande du vice-Premier ministre de l'époque, le *Royal United Services Institute* (« l'Institut royal »), un groupe de réflexion indépendant, a réalisé un contrôle de la surveillance, en partie en réaction aux révélations d'Edward Snowden. L'Institut royal avait pour mandat de vérifier la légalité des programmes de surveillance mis en œuvre par le Royaume-Uni et l'efficacité des régimes qui les encadraient, et de proposer les réformes qui pourraient être nécessaires pour protéger à la fois la vie privée des individus et les capacités que devaient conserver la police et les services de sécurité et de renseignement.

157. Dans son rapport, l'Institut royal déclarait qu'à l'issue de son contrôle, il n'avait décelé aucun élément de nature à indiquer que le gouvernement britannique ait agi de manière délibérément illégale en interceptant des communications privées, ou qu'il ait utilisé la possibilité de collecter des données en masse pour disposer en permanence d'une fenêtre ouverte sur la vie privée des citoyens britanniques. En revanche, il estimait que le cadre juridique autorisant l'interception des communications alors en vigueur n'était pas clair, qu'il n'avait pas suivi l'évolution de la technologie des communications et qu'il n'était satisfaisant ni pour le gouvernement ni pour le public. Il concluait en conséquence qu'il fallait mettre en place un nouveau cadre juridique, complet et plus clair.

158. En particulier, l'Institut royal appuyait l'avis énoncé tant dans le rapport de la commission parlementaire que dans le rapport Anderson selon lequel il fallait certes que les autorités conservent leurs pouvoirs de surveillance, mais aussi qu'un nouveau cadre législatif et un nouveau régime de supervision soient mis en place. Il estimait également que la définition des « données de contenu » et celle des « données de communication » devaient être révisées dans le cadre de l'élaboration de la

nouvelle législation, afin que ces notions soient clairement délimitées par la loi.

159. L'Institut royal observait que pour chaque individu, le volume de données de communication disponible était supérieur au volume de données de contenu, car chaque contenu s'accompagnait de multiples données de communication. Il notait également que l'agrégation d'ensembles de données de communication permettait de brosser un tableau extrêmement précis de la vie d'un individu, car des algorithmes fonctionnant sur des ordinateurs puissants alimentés par un volume suffisant de données brutes pouvaient générer un portrait relativement complet de la personne et de ses habitudes sans même accéder au contenu des données. Il soulignait en outre que l'accès aux données de contenu était de plus en plus difficile en raison de la sophistication croissante des méthodes de cryptage utilisées.

160. L'Institut royal jugeait que la possibilité pour les services de sécurité et de renseignement de collecter et d'analyser en masse des éléments interceptés devait être maintenue, mais encadrée par les garanties renforcées préconisées dans le rapport Anderson. Il considérait lui aussi que les mandats autorisant des interceptions en masse devaient être beaucoup plus détaillés et qu'ils devaient faire l'objet d'un processus d'autorisation judiciaire, sauf en cas d'urgence.

161. Par ailleurs, l'Institut royal faisait siennes les conclusions figurant tant dans le rapport de la commission parlementaire que dans le rapport Anderson selon lesquelles il fallait qu'il y ait différents types de mandat d'interception et d'acquisition des communications et des données associées. Il proposait que les mandats émis à des fins liées à la détection et à la prévention de la criminalité grave et organisée fassent toujours l'objet d'une autorisation délivrée par un commissaire judiciaire, et que les mandats émis à des fins liées à la sécurité nationale fassent l'objet d'une autorisation délivrée par un ministre et soumise au contrôle juridictionnel d'un commissaire judiciaire.

162. L'Institut royal recommandait que l'IPT tienne des audiences publiques, sauf si celui-ci estimait qu'une audience à huis clos s'imposait dans l'intérêt de la justice ou dans un autre intérêt public précis dans telle ou telle affaire. L'Institut royal était également d'avis que l'IPT devait pouvoir vérifier les preuves secrètes produites devant lui, éventuellement en désignant un conseil spécial. Enfin, il déclarait souscrire aux conclusions du rapport de la commission parlementaire et du rapport Anderson soulignant l'importance de la possibilité d'un recours interne contre les décisions de l'IPT et la nécessité d'envisager l'instauration d'un tel recours dans la législation à venir.

5. Le rapport établi à l'issue du contrôle des pouvoirs de surveillance de masse

163. Un contrôle des pouvoirs de surveillance de masse a été réalisé en mai 2016 pour évaluer la justification pratique des quatre pouvoirs de surveillance de masse (interception en masse, acquisition en masse de données de communication, intrusion massive dans les systèmes de communication, constitution d'importantes bases de données à caractère personnel) prévus par ce qui était alors le projet de loi sur les pouvoirs d'enquête (devenu la loi de 2016 sur les pouvoirs d'enquête, paragraphes 183-190 ci-dessous).

164. Comme le contrôle des pouvoirs d'enquête, le contrôle des pouvoirs de surveillance de masse a été mené à bien par le contrôleur indépendant de la législation sur le terrorisme. Pour accomplir sa mission, celui-ci recruta une équipe de trois personnes qui disposaient du niveau d'habilitation de sécurité requis pour accéder à des éléments hautement confidentiels. Cette équipe était composée d'une personne possédant les connaissances techniques nécessaires pour comprendre les systèmes et techniques utilisés par le GCHQ et les utilisations qui pouvaient en être faites, d'un enquêteur qui avait l'expérience de l'utilisation de renseignements secrets et notamment de ceux émanant du GCHQ, et d'un conseil indépendant très qualifié doté des compétences et de l'expérience nécessaires pour vérifier d'un point de vue scientifique et technique les éléments de preuve et les études de cas présentés par les services de sécurité et de renseignement.

165. Dans le cadre de ce contrôle, l'équipe eut des échanges abondants et détaillés avec les services de renseignement à tous les niveaux hiérarchiques ainsi qu'avec les organes de supervision compétents (dont l'IPT et le Conseil près le Tribunal), avec des ONG et avec des experts techniques indépendants.

166. Le contrôle portait sur le projet de loi sur les pouvoirs d'enquête, mais plusieurs des conclusions auxquelles l'équipe a abouti en ce qui concerne l'interception en masse sont pertinentes pour la présente affaire. Notamment, après avoir examiné de nombreux éléments confidentiels, l'équipe a conclu que l'interception en masse constituait un moyen d'action essentiel, d'une part parce que les terroristes, les criminels et les services de renseignement étrangers hostiles disposaient de capacités de plus en plus sophistiquées pour échapper à la détection opérée par des moyens classiques et, d'autre part, parce que la nature mondiale d'Internet avait pour conséquence que la voie empruntée par une communication donnée était devenue fortement imprévisible. Après avoir examiné d'autres techniques que l'interception en masse (notamment les interceptions ciblées, le recours au renseignement humain et l'utilisation d'outils de cyberdéfense commerciaux), l'équipe a conclu qu'aucune d'entre elles, prises isolément

ou combinées, n'aurait été suffisante pour remplacer l'interception en masse en tant que méthode d'obtention des renseignements nécessaires.

6. L'examen indépendant des contrôles internes réalisés au sein du MI5 et des forces de police après les attentats commis à Londres et à Manchester entre mars et juin 2017

167. À la suite d'une série de quatre attentats terroristes commis au Royaume-Uni dans un laps de temps relativement bref (entre mars et juin 2017), au cours duquel 36 innocents trouvèrent la mort et près de 200 autres furent blessés, le ministre de l'Intérieur demanda au contrôleur indépendant de la législation sur le terrorisme récemment retraité, David Anderson, d'examiner les contrôles internes classifiés réalisés au sein des forces de police et des services de renseignement concernés. Le rapport issu de cet examen retraçait ainsi le contexte des attentats :

> « 1.4 Premièrement, le centre conjoint d'analyse du terrorisme [*Joint Terrorism Analysis Centre*] (JTAC) a évalué le ***niveau de menace*** que pose au Royaume-Uni ce que l'on appelle le « terrorisme international » (expression qui désigne en pratique le terrorisme islamiste, qu'il émane du territoire national ou de l'étranger). Il a jugé qu'il était élevé [*SEVERE*] depuis août 2014, ce qui signifie qu'il est « très probable » que des attentats terroristes islamistes aient lieu au Royaume-Uni. Les commentateurs qui ont accès aux renseignements pertinents ont toujours dit clairement que cette évaluation était réaliste. Ils ont souligné également que le terrorisme d'extrême-droite représentait une menace plus réduite mais néanmoins meurtrière, illustrée notamment par l'assassinat de la députée Jo Cox en juin 2016 ou encore l'interdiction du groupe néo-nazi « National Action » en décembre 2016.
>
> 1.5 Deuxièmement, l'***ampleur croissante*** de la menace que représente le terrorisme islamiste est frappante. Le Directeur général du MI5, Andrew Parker, a évoqué en octobre 2017 « une accélération spectaculaire de la menace cette année », au « rythme le plus soutenu qu'[il ait] connu au cours de [ses] 34 années de carrière ». Même si le terrorisme islamiste tue principalement en Afrique, au Moyen-Orient et en Asie du Sud, la menace s'est propagée récemment dans le monde occidental, et elle a été qualifiée de « particulièrement diffuse et diverse au Royaume-Uni ». On ne sait pas encore quels effets, bons ou mauvais, l'effondrement matériel de l'« État islamique » en Syrie et en Irak aura sur cette tendance.
>
> 1.6 Troisièmement, les profils des ***auteurs des attentats*** (...) présentent plusieurs caractéristiques connues (...).
>
> 1.7 Quatrièmement, même si les ***cibles*** des trois premiers attentats ne représentaient pas toute la palette actuelle, elles présentaient des ressemblances importantes avec celles d'autres attentats commis récemment en Occident : centres politiques (Oslo 2011, Ottawa 2014, Bruxelles 2016), concerts, endroits festifs et foule (Orlando 2016, Paris 2016, Barcelone 2017), policiers (Melbourne 2014, Berlin 2015, Charleroi 2016). Il y a aussi eu des cas d'attentats visant des musulmans pratiquants ; le terrorisme s'inscrit alors dans le prolongement des crimes de haine, ce fut le cas par exemple du meurtre de Mohammed Saleem dans les Midlands de l'Ouest en 2013.
>
> 1.8 Cinquièmement, le ***mode opératoire*** des attentats terroristes s'est diversifié et simplifié au fil des années, Daech ayant employé ses formidables efforts de propagande pour inspirer plutôt qu'ordonner la commission d'actes terroristes en

Occident. Les attentats examinés ici étaient typiques par le moment et le lieu où ils ont été commis :

a) Contrairement aux attentats islamistes à grande échelle commis sur ordre, qui étaient typiques de la décennie passée, ces quatre attentats ont été commis par des ***personnes agissant seules*** ou par de ***petits groupes***, et ne présentent guère de signes de préparation soignée ou de ciblage précis.

b) Les armes à feu étant strictement contrôlées au Royaume-Uni, les ***armes blanches*** sont plus fréquemment utilisées que les armes à feu dans les infractions en bande organisée et les infractions terroristes.

c) Depuis qu'un camion a tué 86 innocents à Nice (juillet 2016), les ***véhicules*** – présents dans trois des quatre attentats examinés – sont de plus en plus utilisés comme des armes.

d) C'était déjà par l'***utilisation combinée*** d'un véhicule et d'armes blanches, comme à Westminster et à London Bridge, que le soldat Lee Rigby avait été tué à Woolwich en 2013.

e) Comme à Manchester, les ***explosifs*** ont été l'arme la plus utilisée par les terroristes islamistes qui ont ciblé l'Europe entre 2014 et 2017. L'explosif « TATP » [triperoxyde de triacétone] s'est révélé fabricable (à l'aide d'achats en ligne et d'instructions de réalisation) plus aisément que ce que l'on croyait auparavant. »

7. Le rapport annuel 2016 du Commissaire à l'interception des communications

168. Dans ce rapport, le Commissaire a noté que lorsqu'elle procédait à une interception sur le fondement d'un mandat émis en vertu de l'article 8 § 4 de la RIPA, l'agence interceptrice devait utiliser sa connaissance de l'acheminement des communications internationales ainsi que des études régulières des différentes liaisons de communication pour identifier les canaux de transmission les plus susceptibles de contenir des communications extérieures répondant à la description des éléments sur lesquels portait le certificat ministériel relevant de l'article 8 § 4. Elle devait aussi intercepter les données de manière à limiter la collecte de communications non extérieures au minimum compatible avec le but assigné à l'interception des communications extérieures visées.

169. Le Commissaire a observé également qu'avant que les analystes ne puissent lire, consulter ou écouter des éléments, ils devaient fournir une justification, et notamment préciser la raison pour laquelle ils devaient accéder à ces éléments, conformément à l'article 16 de la RIPA et en vertu du certificat applicable, et pourquoi cet accès était proportionné au but visé. Il a indiqué qu'il ressortait des inspections et des audits que même si la procédure de sélection était suivie soigneusement et consciencieusement, elle reposait sur le jugement professionnel des analystes, sur leur formation et sur la supervision de leur hiérarchie.

170. Selon le rapport, 3007 mandats d'interception avaient été émis en 2016 et cinq demandes avaient été refusées par un ministre. De l'avis du Commissaire, ces chiffres ne faisaient pas apparaître le rôle capital de

contrôle de la qualité exercé en amont par le personnel et les juristes de l'agence interceptrice ou du service de délivrance des mandats (les services de délivrance des mandats fournissaient au ministre des conseils indépendants, et ils examinaient soigneusement les demandes de mandat et les demandes de renouvellement pour veiller à ce que les mesures sollicitées soient – et demeurent – nécessaires et proportionnées au but visé). Sur la base de ses inspections, le Commissaire s'est déclaré convaincu que le faible nombre de demandes rejetées était dû au fait que l'utilisation de ces pouvoirs était mûrement réfléchie.

171. Le rapport exposait que l'inspection d'une agence interceptrice se déroulait normalement de la manière suivante :

- les inspecteurs contrôlaient la mise en œuvre des recommandations et instructions formulées à l'issue de l'inspection précédente ;
- ils évaluaient les systèmes mis en place pour l'interception de communications, afin de s'assurer que ces systèmes étaient adéquats aux fins du chapitre I de la partie I de la RIPA et que toutes les informations pertinentes étaient enregistrées ;
- ils examinaient plusieurs demandes d'interception, afin de vérifier que ces demandes étaient nécessaires et qu'elles répondaient aux exigences de nécessité et de proportionnalité ;
- ils s'entretenaient avec des agents chargés du traitement des affaires, avec des analystes et/ou avec des linguistes ayant participé à certaines enquêtes ou opérations, afin de déterminer si l'interception et la justification de l'acquisition de tous les éléments répondaient aux exigences de proportionnalité ;
- ils examinaient les éventuelles approbations orales urgentes, afin de vérifier que le recours à la procédure d'urgence avait été justifié et approprié ;
- ils examinaient les cas où l'on avait intercepté et conservé des communications protégées par le secret professionnel ou la confidentialité, ainsi que tous les cas où un avocat avait fait l'objet d'une enquête ;
- ils vérifiaient que les garanties et modalités mises en place en vertu des articles 15 et 16 de la RIPA étaient adéquates ;
- ils examinaient les procédures mises en place pour la conservation, le stockage et la destruction des éléments interceptés et des données de communication associées ; et
- ils examinaient les erreurs signalées, et vérifiaient que les mesures mises en place pour empêcher que ces erreurs ne se reproduisent étaient suffisantes.

172. À l'issue de chaque inspection, les inspecteurs établissaient un rapport, qui comprenait :

- une évaluation de la mesure dans laquelle les recommandations de l'inspection précédente avaient été suivies ;
- un récapitulatif du nombre et du type de documents d'interception sélectionnés pour l'inspection, y compris une liste détaillée des mandats ;
- des commentaires détaillés sur tous les mandats sélectionnés pour examen plus approfondi et discussion au cours de l'inspection ;
- une évaluation des erreurs signalées au Commissariat pendant la période couverte par l'inspection ;
- un compte rendu de l'examen des procédures de conservation, de stockage et de destruction ;
- un compte rendu des autres questions politiques ou opérationnelles soulevées par l'agence ou le service de délivrance des mandats pendant l'inspection ;
- une évaluation de la manière dont, le cas échéant, les éléments soumis au secret professionnel des avocats (ou les autres éléments confidentiels) avaient été traités ; et
- un certain nombre de recommandations visant à améliorer le respect du cadre juridique et la performance.

173. En 2016, le commissariat avait inspecté les neuf agences interceptrices une fois et les quatre principaux services de délivrance de mandats deux fois. Ajoutées à ces chiffres, les visites supplémentaires au GCHQ portaient le nombre de visites d'inspection à 22 au total. En outre, le Commissaire et ses inspecteurs avaient réalisé d'autres visites *ad hoc* dans les agences.

174. Selon le rapport, l'inspection des systèmes mis en place pour la demande et la délivrance de mandats d'interception se déroulait normalement en trois étapes. D'abord, pour disposer d'un échantillon représentatif, les inspecteurs sélectionnaient des mandats visant différents types d'infractions et différents types de menaces pour la sécurité nationale, en recherchant en priorité des mandats d'un intérêt particulier ou particulièrement sensibles (tels que ceux qui donnaient lieu à un niveau inhabituel d'intrusion collatérale, ceux qui avait été prolongés pendant longtemps, ceux qui avaient été approuvés oralement, ceux qui avaient abouti à l'interception de communications protégées par le secret ou la confidentialité, ou encore les mandats dits « thématiques »). Ensuite, au cours des jours qui précédaient les inspections, ils examinaient en détail les mandats sélectionnés et les documents associés. À ce stade, les inspecteurs étaient en mesure de contrôler les déclarations relatives à la nécessité et à la proportionnalité de l'accès aux données formulées par les analystes lors de l'ajout d'un sélecteur au système de collecte de données pour examen. Chaque déclaration devait se suffire à elle-même et répondre à l'exigence

générale de respect des priorités en matière de collecte de renseignement. Enfin, ils identifiaient les mandats, opérations ou parties de la procédure pour lesquels il leur fallait des informations ou des précisions complémentaires, et ils organisaient un entretien avec le personnel opérationnel, juridique ou technique concerné. Si nécessaire, ils examinaient plus avant la documentation ou les systèmes concernant ces mandats.

175. Au cours des 22 inspections réalisées en 2016, 970 mandats avaient été examinés, soit 61 % du nombre de mandats en vigueur à la fin de l'année et 32 % du total des nouveaux mandats émis en 2016.

176. La durée de conservation des données n'était pas prévue par la loi, mais les agences devaient se baser sur l'article 15 § 3 de la RIPA, qui disposait que les éléments ou données devaient être détruits dès que leur conservation n'était plus nécessaire dans l'un des buts autorisés par l'article 15 § 4. Selon le rapport, les agences interceptrices avaient toutes un avis différent quant à ce qui constituait une durée de conservation appropriée des éléments interceptés et des données de communication associées. En conséquence, les durées de conservation différaient en fonction des agences interceptrices, s'échelonnant entre trente jours et un an pour les données de contenu, et entre six mois et un an pour les données de communication associées. Toutefois, en pratique, la grande majorité des données de contenu étaient examinées et supprimées automatiquement dans un délai bref, à moins qu'une mesure spécifique ne soit prise pour les conserver plus longtemps parce que cette conservation était nécessaire.

177. Le Commissaire s'est déclaré « impressionné par la qualité » des déclarations relatives à la nécessité et à la proportionnalité de l'accès aux données formulées par les analystes lors des ajouts de sélecteurs au système de collecte de données pour examen.

178. Dans leurs rapports d'inspection, les inspecteurs avaient fait au total 28 recommandations, dont 18 quant à la procédure de demande. La majorité des recommandations relatives à la procédure de demande concernaient la nécessité, la proportionnalité et/ou les justifications avancées dans les demandes à l'appui d'une intrusion collatérale, ou encore le traitement d'éléments protégés par le secret professionnel ou la confidentialité en raison du caractère sensible de la profession du sujet.

179. En 2016, 108 erreurs d'interception au total avaient été signalées au Commissaire. Les causes les plus fréquentes d'erreur d'interception étaient la collecte trop large (en général, il s'agissait d'erreurs techniques au niveau logiciel ou matériel qui aboutissaient à une collecte trop large d'éléments interceptés et de données de communication associées), la sélection et l'examen non autorisés, la diffusion indue, le manquement à annuler une interception, ou encore l'interception de données à la mauvaise adresse ou pour la mauvaise personne.

180. Enfin, le Commissaire a formulé les observations suivantes au sujet de l'échange d'informations :

« Le GCHQ a fourni des détails exhaustifs sur les modalités d'échange permettant aux partenaires du réseau Five Eyes d'accéder depuis leurs propres systèmes aux résultats de ses mandats. Mes inspecteurs ont également rencontré des représentants du réseau Five Eyes et ont assisté à une démonstration de la manière dont les autres membres de ce réseau peuvent demander l'accès aux données du GCHQ. L'accès à ces données est strictement contrôlé et doit être justifié dans les conditions prévues par la législation du pays hôte et les consignes de traitement énoncées dans les garanties prévues aux articles 15 et 16. Pour pouvoir accéder aux données du GCHQ, les analystes du réseau Five Eyes doivent suivre la même formation juridique que les agents du GCHQ. »

8. Le rapport annuel 2016 du Commissaire aux services de renseignement

181. Dans son rapport sur le respect des « lignes directrices à l'intention des agents des services de renseignement et des membres des forces armées concernant la détention et les interrogatoires de détenus à l'étranger, et la transmission et la réception d'informations relatives à ces détenus » (*Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*), le Commissaire aux services de renseignement a formulé les observations suivantes :

« Dans l'exercice de leurs fonctions, les agences collaborent étroitement avec des services de liaison étrangers, avec lesquels elles partagent régulièrement des renseignements et mènent parfois des opérations conjointes. Je suis convaincu que les agences sont attentives aux implications de leur collaboration avec des partenaires dont les activités sont encadrées par des régimes juridiques différents, et j'observe que les membres de [la communauté du renseignement britannique - *the United Kingdom Intelligence Community*] qui travaillent à l'étranger s'efforcent autant que possible d'appliquer les principes du droit britannique.

(...)

Le GCHQ collabore étroitement avec des agents de liaison, avec lesquels il partage régulièrement des renseignements et mène parfois des opérations conjointes. Il s'agit là d'un domaine complexe, tant pour le GCHQ que pour le SIS, dont les agents doivent travailler avec des partenaires dont les activités sont soumises à des règles juridiques différentes, et parfois incompatibles. Je suis impressionné par les efforts déployés par les agents du GCHQ pour obtenir des assurances auprès de leurs partenaires quant au respect des lignes directrices. Je recommande au GCHQ d'envisager de mentionner, dans les documents pertinents, le fait que des règles de droit étranger ont un impact sur les activités de tel ou tel partenaire.

Je suis convaincu que le GCHQ applique consciencieusement les principes énoncés dans les lignes directrices, et je me félicite de constater que les modifications apportées à la formation des agents qui travaillent en roulement 24 heures sur 24 et sept jours sur sept ont encore amélioré la qualité déjà élevée de la procédure de signalement. À cet égard, j'ai observé qu'il arrive parfois aux agents du GCHQ de mettre à jour *a posteriori* le registre relatif aux lignes directrices pour préciser une appréciation ou apporter des détails complémentaires. S'il est important d'enregistrer toutes les informations disponibles, j'ai recommandé au GCHQ veiller à ce que les

éclaircissements complètent l'enregistrement initial sans s'y substituer. Le GCHQ a plus tard confirmé que cette recommandation avait été mise en œuvre.

(...)

Il incombe également au ministre des Affaires étrangères d'exercer un contrôle sur les situations relevant des lignes directrices dans lesquelles les agences souhaitent procéder à un partage d'informations ou à une intervention directe. Je recommande que le ministère des Affaires étrangères et du Commonwealth [*Foreign and Commonwealth Office*] se procure une copie des assurances données au SIS par des partenaires de liaison, et que celles-ci soient mises à la disposition du ministre des Affaires étrangères pour qu'il puisse les examiner lorsqu'il analyse des documents relevant des lignes directrices. »

182. Le contrôle du respect des lignes directrices relève désormais de la compétence du nouveau Commissaire aux pouvoirs d'enquête (*Investigatory Powers Commissioner*). Les lignes directrices sont en cours de réexamen, le Commissaire aux services de renseignement ayant déclaré dans son rapport pour l'année 2015 qu'il « ne pens[ait] pas que les lignes directrices soient fondamentalement défectueuses ou non adaptées au but visé », mais qu'elles « [étaient] en vigueur depuis plusieurs années dans leur forme actuelle et qu'elles [étaient] perfectibles ».

G. La loi de 2016 sur les pouvoirs d'enquête

183. La loi de 2016 sur les pouvoirs d'enquête (*Investigatory Powers Act 2016*, « la loi sur les pouvoirs d'enquête ») a reçu la sanction royale le 29 novembre 2016. La plupart des pouvoirs qui en découlent ayant pris effet en 2018, le nouveau régime mis en place par ce texte est désormais applicable dans une large mesure.

184. En vertu de cette loi, l'émission d'un mandat d'interception en masse – qui peut porter tant sur le « contenu » de communications que sur les « données secondaires » – doit être nécessaire au moins pour la protection de la sécurité nationale (mais aussi, éventuellement, pour la prévention ou la détection des infractions graves, ou la sauvegarde de la prospérité économique du Royaume-Uni dans la mesure où celle-ci relève aussi de l'intérêt de la sécurité nationale). Le mandat doit préciser les « objectifs opérationnels » pour lesquels les données dont il autorise l'acquisition peuvent être sélectionnées pour examen. L'établissement de la liste des « objectifs opérationnels » par les directeurs des services de renseignement fait l'objet de dispositions détaillées. L'inclusion d'un objectif opérationnel dans la liste en question requiert l'approbation du ministre compétent. La liste des objectifs opérationnels doit être communiquée tous les trois mois à la commission parlementaire et réexaminée au moins une fois par an par le Premier ministre.

185. Les demandes de mandats d'interception en masse doivent être faites par le directeur d'un service de renseignement ou au nom de celui-ci. Le pouvoir d'émettre un mandat doit être exercé par le ministre compétent

lui-même, qui doit pour cela tenir compte des principes de nécessité et de proportionnalité. L'émission d'un mandat est soumise à l'autorisation préalable d'un commissaire judiciaire, qui doit mettre en application les principes du contrôle juridictionnel (dispositif dit du « double verrouillage »). L'examen exercé par le commissaire judiciaire doit donc porter sur des questions telles que celles de la justification de l'ingérence au regard de l'exigence de proportionnalité posée par l'article 8 § 2 de la Convention.

186. Les mandats sont valables six mois s'ils n'ont pas été annulés ou renouvelés. Leur renouvellement est soumis à l'approbation d'un commissaire judiciaire.

187. Les mandats doivent avoir pour « objectif principal » la collecte de « communications liées à l'étranger », c'est-à-dire les communications envoyées ou reçues par des individus qui se trouvent hors des îles Britanniques. La sélection pour examen de contenus interceptés ou d'« éléments protégés » est encadrée par la « garantie applicable aux îles Britanniques », selon laquelle les éléments en question ne peuvent à aucun moment être sélectionnés pour examen si l'un quelconque des critères utilisés pour les sélectionner est lié à individu dont on sait qu'il se trouve dans les îles Britanniques à ce moment-là et si l'utilisation de ce critère vise à l'identification du contenu de communications adressées ou destinées à cet individu.

188. La loi de 2016 a également introduit un droit de recours contre les décisions de l'IPT et remplacé le Commissaire à l'interception des communications par un Commissariat aux pouvoirs d'enquête (paragraphe 138 ci-dessus).

189. Plusieurs nouveaux codes de conduite, dont un code de conduite en matière d'interception de communications remanié, sont entrés en vigueur le 8 mars 2018 (paragraphe 102 ci-dessus).

190. La partie 4 de la loi de 2016, entrée en vigueur le 30 décembre 2016, prévoit un pouvoir d'émettre des « avis de conservation » imposant aux opérateurs de télécommunication de conserver des données. Après l'action engagée par Liberty, le Gouvernement admit que cette partie de la loi était, en l'état, incompatible avec les exigences du droit de l'Union européenne. Le texte ne fut toutefois pas modifié et, le 27 avril 2018, la *High Court* le jugea incompatible avec les droits fondamentaux protégés par le droit de l'Union européenne car, en matière de justice pénale, l'accès aux données conservées n'était pas limité au but de lutter contre les « infractions graves » et, de manière générale, l'accès aux données conservées n'était pas soumis au contrôle préalable d'un tribunal ou d'une instance administrative indépendante.

II. LE DROIT INTERNATIONAL PERTINENT

A. Nations unies

191. La résolution nº 68/167, adoptée par l'Assemblée générale le 18 décembre 2013, est ainsi libellée :

« *L'Assemblée générale*,

(...)

4. *Invite* tous les États :

(...)

c) À revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en veillant à respecter pleinement toutes leurs obligations au regard du droit international ;

d) À créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà ;

(...) »

B. Conseil de l'Europe

1. *La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981)*

192. Cette Convention, qui est entrée en vigueur à l'égard du Royaume-Uni le 1er décembre 1987, pose des normes en matière de protection des données dans le domaine du traitement automatique des données à caractère personnel dans les secteurs public et privé. En ses parties pertinentes, elle prévoit ceci :

Préambule

« Les États membres du Conseil de l'Europe, signataires de la présente Convention,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres, dans le respect notamment de la prééminence du droit ainsi que des droits de l'homme et des libertés fondamentales ;

Considérant qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés ;

Réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières ;

Reconnaissant la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples,

Sont convenus de ce qui suit : »

Article 1er - Objet et but

« Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données »).

(...) »

Article 8 - Garanties complémentaires pour la personne concernée

« Toute personne doit pouvoir :

a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ;

b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ;

c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention ;

d. disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article. »

Article 9 - Exceptions et restrictions

« 1. Aucune exception aux dispositions des articles 5, 6 et 8 de la présente Convention n'est admise, sauf dans les limites définies au présent article.

2. Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique :

a. à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;

b. à la protection de la personne concernée et des droits et libertés d'autrui.

(...) »

Article 10 - Sanctions et recours

« Chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre. »

193. Le rapport explicatif de la convention susmentionnée expose notamment ce qui suit :

Article 9 - Exceptions et restrictions

« 55. Les exceptions aux principes de base pour la protection des données sont limitées à celles nécessaires pour la protection des valeurs fondamentales dans une société démocratique. Le texte du deuxième paragraphe de cet article a été inspiré par celui des deuxièmes paragraphes des articles 6, 8, 10 et 11 de la Convention européenne des Droits de l'Homme. Il ressort des décisions de la Commission et de la Cour des Droits de l'Homme concernant la notion de "mesure nécessaire" que les critères pour une telle notion ne peuvent pas être fixés pour tous les pays et tous les temps, mais qu'il y a lieu de les considérer par rapport à une situation donnée de chaque pays.

56. La lettre a du paragraphe 2 énumère les intérêts majeurs de l'État qui peuvent exiger des exceptions. Ces exceptions ont été formulées de façon très précise pour éviter qu'en ce qui concerne l'application générale de la Convention les États aient une marge de manœuvre trop large.

Les États conservent, aux termes de l'article 16, la faculté de refuser l'application de la Convention dans des cas individuels pour des motifs majeurs y compris ceux énumérés à l'article 9.

La notion de « sécurité de l'État » doit être entendue dans le sens traditionnel de protection de sa souveraineté nationale contre des menaces tant internes qu'externes y compris la protection des relations internationales de l'État. »

2. *Le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (8 novembre 2001, STCE n° 181)*

194. Les dispositions pertinentes de ce protocole, qui n'a pas été ratifié par le Royaume-Uni, se lisent ainsi :

Article 1 – Autorités de contrôle

« 1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole.

2. a. À cet effet, ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 de l'article 1 du présent Protocole.

b. Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence.

3. Les autorités de contrôle exercent leurs fonctions en toute indépendance.

4. Les décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

(...) »

Article 2 – Flux transfrontières de données à caractère personnel vers un destinataire n'étant pas soumis à la juridiction d'une Partie à la Convention

« 1. Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet État ou cette organisation assure un niveau de protection adéquat pour le transfert considéré.

2. Par dérogation au paragraphe 1 de l'article 2 du présent Protocole, chaque Partie peut autoriser un transfert de données à caractère personnel :

a. si le droit interne le prévoit :

– pour des intérêts spécifiques de la personne concernée, ou

– lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou

b. si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne. »

3. La recommandation Comité des Ministres du Conseil de l'Europe sur la protection des données à caractère personnel dans le domaine des services de télécommunication

195. La recommandation n° R (95) 4 du Comité des Ministres, adoptée le 7 février 1995, énonce ce qui suit en ses parties pertinentes :

« 2.4. Il ne peut y avoir ingérence des autorités publiques dans le contenu d'une communication, y compris l'utilisation de tables d'écoute ou d'autres moyens de surveillance ou d'interception des communications, que si cette ingérence est prévue par la loi et constitue une mesure nécessaire, dans une société démocratique :

a. à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;

b. à la protection de la personne concernée et des droits et libertés d'autrui.

2.5. En cas d'ingérence des autorités publiques dans le contenu d'une communication, le droit interne devrait réglementer :

a. l'exercice des droits d'accès et de rectification par la personne concernée ;

b. les conditions dans lesquelles les autorités publiques compétentes seront en droit de refuser de donner des renseignements à la personne concernée ou d'en différer la délivrance ;

c. la conservation ou la destruction de ces données.

Lorsqu'un exploitant de réseau ou un fournisseur de services est chargé par une autorité publique d'effectuer une ingérence, les données ainsi collectées ne devraient être communiquées qu'à l'organisme désigné dans l'autorisation pour cette ingérence. »

4. Le rapport 2015 de la Commission européenne pour la démocratie par le droit (« Commission de Venise ») sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique

196. Dans ce rapport, la Commission de Venise a noté d'emblée la valeur que pouvait présenter l'interception en masse pour les opérations de sécurité, observant que cette méthode permettait aux services de sécurité d'agir en amont, en recherchant des dangers jusque-là inconnus plutôt que d'enquêter sur des dangers connus. Toutefois, elle a aussi noté que le fait d'intercepter des données en masse au cours de leur transmission ou d'ordonner à une société de télécommunications de stocker puis de communiquer aux agences des forces de l'ordre ou des services de sécurité le contenu ou les métadonnées des données de télécommunications portait atteinte aux droits de l'homme et notamment au droit à la vie privée d'une grande partie de la population mondiale. À cet égard, elle a considéré que la principale ingérence dans la vie privée survenait lorsque les agences accédaient aux données personnelles stockées et/ou les traitaient. Pour cette raison, elle a estimé qu'il était important de recourir à l'analyse informatique (généralement réalisée à l'aide de sélecteurs) pour ménager un juste équilibre entre le souci de protéger l'intégrité personnelle et les autres intérêts.

197. La Commission a considéré que les deux garanties les plus importantes résidaient dans le processus d'autorisation (de la collecte et de l'accès aux données collectées) et dans la supervision de celui-ci. Elle a estimé qu'il ressortait nettement de la jurisprudence de la Cour que le processus de supervision devait être confié à un organe indépendant et extérieur. Elle a noté que si la Cour avait montré une préférence pour le système d'autorisation juridictionnelle, elle n'avait pas dit que ce fût une obligation mais elle avait jugé qu'il fallait évaluer le système dans son ensemble et que, en l'absence de contrôles indépendants au stade de l'autorisation, il devait y avoir des garanties extrêmement solides au stade de la supervision. À cet égard, la Commission a examiné l'exemple du système américain, où l'autorisation est donnée par la FISC. Elle a noté que même si ce système requérait l'obtention d'une autorisation juridictionnelle, il ne prévoyait pas de supervision indépendante du suivi des conditions et des limitations énoncées par la juridiction en question, ce qu'elle a estimé problématique.

198. La Commission a indiqué par ailleurs que l'article 8 de la Convention n'imposait pas expressément de notifier aux intéressés qu'ils avaient fait l'objet d'une surveillance, puisque lorsque le droit interne prévoyait une procédure générale de recours devant un organe de supervision indépendant, ce mécanisme pouvait compenser l'absence de notification.

199. Elle a aussi estimé que les contrôles internes constituaient la « principale garantie », que le recrutement et la formation revêtaient une importance clé et qu'il était indispensable que les agences concernées tiennent compte de la protection de la vie privée et des autres droits de l'homme lorsqu'elles promulguaient des règles internes.

200. Elle a reconnu que les journalistes constituaient un groupe méritant une protection spéciale, puisqu'en cherchant dans leurs contacts, on pouvait découvrir leurs sources, ce qui risquait d'avoir un effet fortement dissuasif sur les lanceurs d'alerte potentiels. Elle a néanmoins estimé qu'on ne pouvait édicter une interdiction absolue de recherche dans les contacts d'un journaliste en présence de fortes raisons de recourir à une telle pratique. Elle a admis par ailleurs qu'il était difficile de définir la profession de journaliste, les ONG vouées à la formation de l'opinion publique ou même les blogueurs pouvant selon elle revendiquer à juste titre des protections équivalentes.

201. Enfin, elle a examiné brièvement la question du partage de renseignements, et en particulier le risque que les États utilisent cette pratique pour contourner des procédures internes plus strictes applicables en matière de surveillance et/ou les éventuelles limitations légales auxquelles leurs agences pourraient être soumises en matière d'opérations relevant du renseignement intérieur. Pour parer à ce risque, elle a estimé qu'il serait utile de prévoir que les données transférées en masse ne puissent faire l'objet d'une analyse que si les conditions matérielles pesant sur toute investigation au niveau national étaient réunies et si l'agence de collecte de renseignements d'origine électromagnétique avait obtenu les mêmes autorisations que celles requises pour une analyse de données de masse réalisée avec ses propres techniques.

III. LE DROIT DE L'UNION EUROPÉENNE

A. La Charte des droits fondamentaux de l'Union européenne

202. Les articles 7, 8 et 11 de la charte sont ainsi libellés :

Article 7 – Respect de la vie privée et familiale

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

Article 8 – Protection des données à caractère personnel

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

Article 11 – Liberté d'expression et d'information

« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés. »

B. Les directives et règlements de l'Union européenne relatifs à la protection et au traitement des données personnelles

203. La directive sur la protection des données à caractère personnel (directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), adoptée le 24 octobre 1995, a régi pendant des années la protection et le traitement des données à caractère personnel au sein de l'Union européenne. Elle ne s'appliquait toutefois pas aux activités des États membres concernant la sécurité publique, la défense et la sûreté de l'État, celles-ci ne relevant pas du champ d'application du droit communautaire (article 3 § 2).

204. Le règlement général sur la protection des données (RGPD), adopté en avril 2016, a remplacé la directive sur la protection des données. Il est entré en vigueur le 25 mai 2018, et est d'application directe dans les États membres[2]. Il renferme des dispositions et des garanties relatives au traitement au sein de l'Union européenne des informations permettant d'identifier personnellement les personnes qu'elles concernent. Il s'applique à toutes les entreprises qui ont des activités dans l'Espace économique européen, quel que soit l'endroit où elles se trouvent. Il prévoit que les processus opérationnels dans le cadre desquels sont traitées des données personnelles doivent assurer la protection des données dès la conception et par défaut. Ainsi, les données personnelles doivent, avant d'être stockées, faire l'objet d'une pseudonymisation voire d'une anonymisation totale, et les paramètres par défaut doivent être ceux qui assurent le plus grand respect de la vie privée, afin que les données ne soient pas disponibles publiquement sans le consentement exprès de la personne concernée et qu'elles ne puissent pas être utilisées pour identifier la personne en l'absence d'informations supplémentaires conservées séparément. Aucune donnée personnelle ne peut être traitée autrement que sur une base légale prévue par le règlement ou sur accord express par adhésion du titulaire des données, recueilli par celui qui procède au traitement des données ou par

[2] Avant le retrait du Royaume-Uni de l'Union européenne, la sanction royale a été donnée le 23 mai 2018 à la loi de 2018 sur la protection des données, qui renferme des dispositions et garanties équivalentes.

celui qui en est responsable. Le titulaire des données a le droit de révoquer cette permission à tout moment.

205. Quiconque traite des données personnelles doit clairement avertir qu'il recueille des données, mentionner la base légale sur laquelle il agit et le but du traitement des données ainsi que la durée pendant laquelle celles-ci seront conservées et, le cas échéant, le fait qu'elles sont partagées avec des tiers ou des acteurs externes à l'Union européenne. L'utilisateur a le droit de demander une copie dans un format courant et interopérable des données collectées aux fins de traitement, et le droit à ce que ses données soient effacées dans certaines circonstances. Les autorités publiques et les entreprises dont les activités sont centrées sur le traitement régulier ou systématique des données personnelles sont tenues d'employer un délégué à la protection des données chargé d'assurer le respect du RGPD. Les entreprises doivent signaler les éventuelles violations des données dans un délai de 72 heures si ces violations ont un effet négatif sur le respect de la vie privée des utilisateurs.

206. La directive vie privée et communications électroniques (directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques), adoptée le 12 juillet 2002, énonce ceci dans ses considérants 2 et 11 :

> « 2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la charte des droits fondamentaux de l'Union européenne. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.
>
> (...)
>
> 11) À l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. »

207. Les dispositions pertinentes de cette directive se lisent ainsi :

Article premier – Champ d'application et objectif

« 1. La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal. »

Article 15 – Application de certaines dispositions de la directive 95/46/CE

« 1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

208. La directive sur la conservation des données (directive 2006/24/CE 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, et modifiant la directive 2002/58/CE) a été adoptée le 15 mars 2006. Avant l'arrêt de 2014 qui l'a déclarée invalide (paragraphe 209 ci-dessous), elle disposait notamment ce qui suit :

Article premier - Objet et champ d'application

« 1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

2. La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques. »

Article 3 – Obligation de conservation de données

« 1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans leur ressort. »

C. La jurisprudence pertinente de la Cour de justice de l'Union européenne (« la CJUE »)

1. Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a. *(affaires jointes C-293/12 et C-594/12 ; ECLI:EU:C:2014:238)*

209. Par un arrêt du 8 avril 2014, la CJUE a déclaré invalide la directive 2006/24/CE sur la conservation des données, qui obligeait les fournisseurs de services de communications électroniques accessibles au public ou les réseaux publics de communications à conserver toutes les données relatives au trafic et les données de localisation pour une durée de six mois à deux ans de manière à ce que ces données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne. Elle a noté que, même si la directive n'autorisait pas la conservation du contenu des communications, les données relatives au trafic et les données de localisation qu'elle visait étaient susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données avaient été conservées. Elle en a déduit que l'obligation de conserver ces données constituait en elle-même une ingérence dans le droit au respect de la vie privée et des communications et dans le droit à la protection des données à caractère personnel garantis respectivement par l'article 7 et par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

210. Elle a jugé également que l'accès des autorités nationales compétentes aux données constituait une ingérence supplémentaire dans ce droit fondamental, et que cette ingérence était « particulièrement grave ». Elle a considéré que la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci étaient effectuées sans que l'abonné ou l'utilisateur inscrit en fussent informés était susceptible de générer dans

l'esprit des personnes concernées le sentiment que leur vie privée faisait l'objet d'une surveillance constante. Elle a conclu que l'ingérence répondait à un objectif d'intérêt général, à savoir contribuer à la lutte contre la criminalité grave et le terrorisme et ainsi, en fin de compte, à la sécurité publique, mais qu'elle ne respectait pas le principe de proportionnalité.

211. En premier lieu, la directive couvrait 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 ne soient opérées en fonction de l'objectif de lutte contre les infractions graves. Elle comportait donc, selon la CJUE, une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne. Elle s'appliquait même à des personnes pour lesquelles il n'existait aucun indice de nature à laisser croire que leur comportement pût avoir un lien, même indirect ou lointain, avec des infractions graves.

212. En deuxième lieu, la directive ne contenait pas les conditions matérielles et procédurales afférentes à l'accès des autorités nationales compétentes aux données et à l'utilisation ultérieure de ces données : elle visait simplement, de manière générale, les infractions graves telles que définies par chaque État membre dans son droit interne, mais elle ne prévoyait aucun critère objectif permettant de déterminer quelles infractions pouvaient être considérées comme suffisamment graves pour justifier une ingérence aussi poussée dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte. Surtout, l'accès aux données par les autorités nationales compétentes n'était pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision aurait visé à limiter l'accès aux données et leur utilisation à ce qui serait strictement nécessaire aux fins d'atteindre l'objectif poursuivi.

213. En troisième lieu, la directive imposait la conservation de toutes les données pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. La CJUE a donc conclu que la directive comportait une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, sans que cette ingérence ne soit précisément encadrée par des dispositions permettant de garantir qu'elle serait effectivement limitée au strict nécessaire. Elle a considéré également que la directive ne prévoyait pas de garanties permettant d'assurer, par des mesures techniques et organisationnelles, une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites.

2. Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. *(affaires jointes C-203/15 et C-698/15 ; ECLI:EU:C:2016:970)*

214. Dans l'affaire *Secretary of State for the Home Department contre Tom Watson e.a.*, les requérants avaient sollicité le contrôle juridictionnel de la légalité de l'article 1er de la loi de 2014 sur la conservation des données et les pouvoirs d'enquête (*Data Retention and Investigatory Powers Act 2014*, « la DRIPA »), en vertu duquel le ministre de l'Intérieur pouvait, s'il estimait cette mesure nécessaire et proportionnée à un ou plusieurs des buts visés aux alinéas a) à h) de l'article 22 § 2 de la RIPA, ordonner à un opérateur de télécommunications publiques de conserver des données de communication. Les requérants soutenaient notamment que cet article était incompatible avec les articles 7 et 8 de la Charte et avec l'article 8 de la Convention.

215. Le 17 juillet 2015, la *High Court* avait jugé que l'arrêt rendu par la CJUE dans l'affaire *Digital Rights* énonçait des « exigences impératives en droit de l'Union » applicables à la législation des États membres relative à la conservation des données de communication et à l'accès à ces données. Elle avait estimé que, dès lors que la CJUE avait dit dans cet arrêt que la directive 2006/24 était incompatible avec le principe de proportionnalité, un texte national au contenu identique à celui de cette directive ne pouvait pas non plus être compatible avec ce principe. Selon la *High Court*, il découlait de la logique sous-tendant l'arrêt *Digital Rights* qu'une législation établissant un régime généralisé de conservation des données de communication était contraire aux droits garantis aux articles 7 et 8 de la Charte si elle n'était pas complétée par un régime d'accès aux données défini par le droit national et prévoyant des garanties suffisantes pour la sauvegarde de ces droits, et dès lors, l'article 1er de la DRIPA n'était pas compatible avec les articles 7 et 8 de la Charte puisqu'il n'établissait pas de règles claires et précises relatives à l'accès aux données conservées et à l'utilisation de ces données et il ne subordonnait pas l'accès à ces données au contrôle préalable d'une juridiction ou d'une instance administrative indépendante.

216. Le ministre de l'Intérieur ayant contesté devant la *Court of Appeal* la décision de la *High Court*, la *Court of Appeal* sollicitait de la CJUE une décision préjudicielle.

217. Devant la CJUE, l'affaire *Secretary of State for the Home Department contre Tom Watson e.a.* fut jointe à l'affaire C-203/15, *Tele2 Sverige AB contre Post- och telestyrelsen*, dans laquelle la cour administrative d'appel de Stockholm (*Kammarrätten i Stockholm*) sollicitait une décision préjudicielle. À la suite d'une audience à laquelle une quinzaine d'États membres de l'Union européenne intervinrent, la CJUE rendit son arrêt, le 21 décembre 2016. Elle conclut que l'article 15 § 1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de

l'article 52, paragraphe 1, de la Charte, devait être interprété en ce sens qu'il s'opposait à l'existence d'une législation nationale régissant la protection et la sécurité des données de trafic et des données de localisation, y compris l'accès des autorités nationales compétentes aux données conservées, qui ne restreindrait pas l'accès à ces données dans le cadre de la lutte contre la criminalité aux fins de la seule lutte contre la criminalité grave, qui ne soumettrait pas cet accès au contrôle préalable d'un tribunal ou d'une autorité administrative indépendante, et qui n'imposerait pas que les données concernées soient conservées sur le territoire de l'Union.

218. La CJUE déclara par ailleurs irrecevable la question, posée par la *Court of Appeal*, de savoir si la protection conférée par les articles 7 et 8 de la Charte allait au-delà de celle garantie par l'article 8 de la Convention.

219. Après que la CJUE eut rendu cet arrêt, l'affaire revint devant la *Court of Appeal*. Le 31 janvier 2018, celle-ci rendit une décision de redressement déclaratoire selon laquelle l'article 1er de la DRIPA était incompatible avec le droit de l'Union européenne dans la mesure où il permettait d'accéder aux données conservées sans que cet accès ne soit limité aux seules fins de lutte contre la criminalité grave ni soumis au contrôle préalable d'un tribunal ou d'une autorité administrative indépendante.

3. Ministerio Fiscal *(affaire C-207/16; ECLI:EU:C:2018:788)*

220. La demande de décision préjudicielle en cause dans cette affaire avait été introduite devant la CJUE après que la police espagnole, qui enquêtait sur le vol d'un portefeuille et d'un téléphone mobile, eut demandé à un juge d'instruction l'accès aux données permettant d'identifier les utilisateurs de numéros de téléphone activés pendant la période de douze jours ayant précédé le vol. Le juge d'instruction avait rejeté cette demande, au motif notamment que les faits objet de l'enquête n'étaient pas constitutifs d'une infraction « grave ». La juridiction de renvoi demandait à la CJUE de lui fournir des indications sur la fixation du seuil de gravité des infractions à partir duquel une ingérence dans les droits fondamentaux, telle que l'accès par les autorités nationales compétentes aux données à caractère personnel conservées par les fournisseurs de services de communications électroniques, pouvait être justifiée.

221. Par un arrêt du 2 octobre 2018, la Grande Chambre de la CJUE a jugé que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, devait être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires de cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, s'analysait en une ingérence dans les droits fondamentaux de ces derniers qui ne présentait pas une gravité telle que cet accès dût être limité, en matière de prévention, de recherche, de

détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave. Elle a notamment précisé ce qui suit :

> « En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ».
>
> En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général. »

222. Elle a considéré que l'accès aux données visées par la demande en cause ne constituait pas une ingérence particulièrement grave, au motif que ces données

> « permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées. »

4. Maximillian Schrems contre Data Protection Commissioner *(affaire C-362/14 ; ECLI:EU:C:2015:650)*

223. La demande de décision préjudicielle en cause dans cette affaire avait été présentée devant la CJUE après l'introduction d'une plainte contre Facebook Ireland Ltd introduite auprès du Commissaire à la protection des données (*Data Protection Commissioner*) par M. Schrems, un citoyen autrichien militant pour la défense de la vie privée. Ce dernier se plaignait du transfert de ses données à caractère personnel vers les États-Unis par Facebook Ireland et de leur conservation sur des serveurs situés dans ce pays. Le Commissaire à la protection des données avait rejeté la plainte de M. Schrems au motif que, par une décision du 26 juillet 2000 (relative à la « sphère de sécurité »), la Commission européenne avait jugé que les États-Unis garantissaient un niveau de protection adéquat aux données à caractère personnel transférées.

224. Par un arrêt du 6 octobre 2015, la CJUE a jugé que l'existence d'une décision de la Commission constatant qu'un pays tiers assure un niveau de protection adéquat aux données à caractère personnel transférées ne pouvait annihiler ni même réduire les pouvoirs dont disposent les autorités nationales de contrôle en vertu de la Charte et de la directive sur le traitement des données à caractère personnel. Ainsi, même en présence d'une décision de la Commission, les autorités nationales de contrôle

doivent pouvoir examiner en toute indépendance si le transfert des données d'une personne vers un pays tiers respecte les exigences posées par la directive.

225. Néanmoins, la CJUE a rappelé qu'elle était seule compétente pour constater l'invalidité d'une décision de la Commission. À cet égard, elle a relevé que le régime de la sphère de sécurité n'était applicable qu'aux entreprises qui y avaient souscrit, sans que les autorités publiques des États-Unis y soient elles-mêmes soumises. En outre, elle a relevé que les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis l'emportaient sur le régime de la sphère de sécurité, si bien que les entreprises américaines étaient tenues d'écarter, sans limitation, les règles de protection prévues par ce régime, lorsqu'elles entraient en conflit avec de telles exigences. Elle a constaté que le régime américain de la sphère de sécurité rendait ainsi possible des ingérences, par les autorités publiques américaines, dans les droits fondamentaux des personnes, la décision de la Commission relative à la sphère de sécurité ne faisant état ni de l'existence, aux États-Unis, de règles destinées à limiter ces éventuelles ingérences ni de l'existence d'une protection juridique efficace contre ces ingérences.

226. En ce qui concerne la question de savoir si le niveau de protection garanti aux États-Unis était substantiellement équivalent aux libertés et droits fondamentaux garantis au sein de l'Union, la CJUE a constaté que la réglementation en vigueur dans l'Union n'était pas limitée au strict nécessaire, dès lors qu'elle autorisait de manière généralisée la conservation de toutes les données à caractère personnel de toutes les personnes dont les données étaient transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception ne soient opérées en fonction de l'objectif poursuivi et sans que des critères objectifs ne soient prévus en vue de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure. Elle a ajouté qu'une règlementation européenne permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques devait être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée. De même, elle a relevé qu'une règlementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, portait atteinte au contenu essentiel du droit fondamental à une protection juridictionnelle effective.

227. Enfin, elle a jugé que la décision relative à la sphère de sécurité privait les autorités nationales de contrôle de leurs pouvoirs, dans le cas où une personne aurait remis en cause la compatibilité de cette décision avec la protection de la vie privée et des libertés et droits fondamentaux des personnes. Estimant que la Commission n'avait pas la compétence de

restreindre ainsi les pouvoirs des autorités nationales de contrôle, la CJUE a jugé que la décision relative à la sphère de sécurité était invalide.

5. Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems *(affaire C-311/18; ECLI:EU:C:2020:559)*

228. À la suite de l'arrêt rendu par la CJUE le 6 octobre 2015, la juridiction de renvoi avait annulé le rejet de la plainte introduite par M. Schrems, qu'elle avait renvoyée devant le Commissaire à la protection des données. Dans le cadre de l'enquête ouverte par ce dernier, Facebook Ireland avait expliqué qu'une grande partie des données à caractère personnel était transférée à Facebook Inc. sur le fondement des clauses types de protection des données figurant à l'annexe de la décision 2010/87/UE de la Commission, telle que modifiée.

229. Dans sa plainte reformulée, M. Schrems avait allégué notamment que le droit américain imposait à Facebook Inc. de mettre les données à caractère personnel qui lui avaient été transférées à la disposition de certaines autorités américaines, telles que la NSA et le Bureau fédéral d'enquête (*Federal Bureau of Investigation*, « le FBI »). Il avait soutenu que ces données étant utilisées dans le cadre de différents programmes de surveillance d'une manière incompatible avec les articles 7, 8 et 47 de la Charte, la décision 2010/87/UE ne pouvait justifier le transfert desdites données vers les États-Unis. Dans ces conditions, M. Schrems avait demandé au Commissaire d'interdire ou de suspendre le transfert de ses données à caractère personnel vers Facebook Inc.

230. Le 24 mai 2016, le Commissaire avait publié un projet de décision dans lequel il avait considéré provisoirement que les données à caractère personnel des citoyens de l'Union transférées vers les États-Unis risquaient d'être consultées et traitées par les autorités américaines d'une manière incompatible avec les articles 7 et 8 de la Charte, et que le droit des États-Unis n'offrait pas à ces citoyens des voies de recours compatibles avec l'article 47 de la Charte. Le Commissaire avait estimé que les clauses types de protection des données figurant à l'annexe de la décision 2010/87/UE n'étaient pas de nature à remédier à ce défaut, car elles ne liaient pas les autorités américaines.

231. Après examen des activités des services de renseignement américains autorisées par l'article 702 de la FISA et le décret présidentiel nº 12333 (*Executive Order 12333*), la *High Court* avait conclu que les États-Unis procédaient à un traitement de données en masse sans assurer une protection substantiellement équivalente à celle garantie par les articles 7 et 8 de la Charte, et que les citoyens de l'Union n'avaient pas accès aux mêmes recours que ceux dont disposaient les ressortissants américains. Elle en avait déduit que le droit américain n'assurait pas aux citoyens de l'Union un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré à l'article 47 de la Charte. Elle avait sursis à

statuer et posé plusieurs questions préjudicielles à la CJUE. Dans son renvoi préjudiciel, elle demandait notamment à la CJUE de se prononcer sur la question de savoir si le droit de l'Union était applicable au transfert de données, par une société privée d'un État membre de l'Union, à une société privée établi dans un pays tiers et, dans l'affirmative, comment il convenait d'évaluer le niveau de protection garanti par le pays tiers. Elle lui demandait également de statuer sur le point de savoir si le niveau de protection garanti par les États-Unis respectait la substance des droits protégés par l'article 47 de la Charte.

232. Dans son arrêt du 16 juillet 2020, la CJUE a constaté que le règlement général sur la protection des données (« RGPD ») s'appliquait au transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, nonobstant le fait que, au cours ou à la suite de ce transfert, ces données étaient susceptibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'État. En outre, elle a jugé que les garanties appropriées, les droits opposables et les voies de droit effectives requis par le RGDP devaient assurer que les droits des personnes dont les données à caractère personnel étaient transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficiaient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne. À cet effet, elle a déclaré que l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert devait prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union européenne et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concernait un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci.

233. Par ailleurs, elle a dit que, sauf s'il existait une décision d'adéquation valablement adoptée par la Commission européenne, l'autorité de contrôle compétente était tenue de suspendre ou d'interdire un transfert de données vers un pays tiers lorsque celle-ci considérait, à la lumière de l'ensemble des circonstances propres à ce transfert, que les clauses types de protection des données adoptées par la Commission n'étaient pas ou ne pouvaient pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union ne pouvait pas être assurée par d'autres moyens.

234. Elle a précisé que l'adoption, par la Commission, d'une décision d'adéquation exigeait la constatation dûment motivée, de la part de cette institution, que le pays tiers concerné assurait effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui

garanti dans l'ordre juridique de l'Union. Elle a constaté que la décision relative à la sphère de sécurité était invalide. Elle a relevé que l'article 702 de la FISA ne faisait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'il comportait pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur, pas plus que l'existence de garanties pour des personnes non américaines potentiellement visées par ces programmes. Dans ces conditions, elle a conclu que cet article n'était pas susceptible d'assurer un niveau de protection substantiellement équivalent à celui garanti par la Charte. S'agissant des programmes de surveillance fondés sur le décret présidentiel n° 12333, elle a considéré que ce décret ne conférait pas non plus de droits opposables aux autorités américaines devant les tribunaux.

6. Privacy International contre Secretary of State for Foreign and Commonwealth Affairs e.a. *(C-623/17; ECLI:EU:C:2020:790) et* La Quadrature du Net e.a., French Data Network e.a. et Ordre des barreaux francophones et germanophone e.a. *(affaires jointes C 511/18, C-512/18 et C-520/18; ECLI:EU:C:2020:791)*

235. Le 8 septembre 2017, l'IPT statua dans l'affaire *Privacy International*, qui concernait l'acquisition par les services de renseignement, en vertu de l'article 94 de la loi de 1984 sur les télécommunications (*Telecommunications Act 1984*), de données de communication en masse et de données personnelles en masse. Il estima que, puisque leur existence avait été reconnue, ces régimes d'acquisition de données étaient conformes à l'article 8 de la Convention. Il énonça toutefois quatre exigences, qui découlaient apparemment de l'arrêt rendu par la CJUE dans l'affaire *Watson et autres*, et qui semblaient aller au-delà des exigences de l'article 8 de la Convention : la restriction de l'accès aux données de masse non ciblées, la nécessité d'une autorisation préalable (sauf en cas d'urgence dûment établie) à l'accès aux données, l'existence de mesures prévoyant la notification ultérieure des personnes concernées et la conservation de toutes les données sur le territoire de l'Union européenne.

236. Le 30 octobre 2017, l'IPT adressa une demande de décision préjudicielle à la CJUE, afin que celle-ci précise la mesure dans laquelle les exigences posées dans l'arrêt *Watson* seraient applicables dans le cas où l'acquisition de données en masse et le recours à des techniques de traitement automatisé seraient nécessaires pour protéger la sécurité nationale. Dans cette demande, il exprimait de fortes préoccupations pour le cas où la CJUE considérerait que les exigences *Watson* étaient effectivement applicables aux mesures prises pour protéger la sécurité nationale : il estimait que cela aurait fait échec à ces mesures et mis en péril la sécurité nationale des États membres. Il affirmait que l'acquisition en masse présentait des avantages pour la protection de la sécurité nationale, que l'exigence d'une autorisation préalable risquerait de porter atteinte à la

capacité des services de renseignement à faire face aux menaces pour la sécurité nationale, qu'il serait dangereux et difficile en pratique d'appliquer une exigence d'avertissement à l'égard de l'acquisition ou de l'utilisation de données en masse, en particulier lorsque la sécurité nationale était en jeu, et qu'une interdiction absolue de transférer ces données hors de l'Union européenne risquerait d'avoir un impact sur les obligations internationales conventionnelles des États membres.

237. La CJUE tint une audience publique le 9 septembre 2019. Elle examina l'affaire *Privacy International* en même temps que les affaires jointes C‑511/18 et C‑512/18 – *La Quadrature du Net et autres*, et C‑520/18 – *Ordre des barreaux francophones et germanophone et autres*, qui portaient elles aussi sur l'application de la directive 2002/58 aux activités liées à protection de la sécurité nationale et à la lutte contre le terrorisme. Treize États intervinrent au soutien de l'État concerné.

238. Le 6 octobre 2020, la CJUE rendit deux arrêts distincts. Dans l'affaire *Privacy International*, elle jugea qu'une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale relevait du champ d'application de la directive « vie privée et communications électroniques ». Elle déclara que l'interprétation de cette directive devait tenir compte du droit au respect de la vie privée, garanti à l'article 7 de la Charte, du droit à la protection des données à caractère personnel, garanti à l'article 8 du même texte, ainsi que du droit à la liberté d'expression, garanti à l'article 11. Elle précisa que les limitations à l'exercice de ces droits devaient être prévues par la loi, qu'elles devaient respecter le contenu essentiel desdits droits et le principe de proportionnalité, et qu'elles devaient être nécessaires et répondre effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Elle ajouta que les limitations à la protection des données à caractère personnel devaient s'opérer dans les limites du strict nécessaire et que, pour satisfaire à l'exigence de proportionnalité, une réglementation devait prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel étaient concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus.

239. Elle considéra qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée – qui touchait l'ensemble des personnes faisant usage de services de communications électroniques – des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement excédait les limites du strict

nécessaire, et qu'elle ne pouvait être considérée comme étant justifiée au regard de la directive « vie privée et communications électroniques » lue à la lumière de la Charte.

240. Toutefois, dans l'affaire *La Quadrature du Net et autres*, la CJUE précisa que si la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'opposait à des mesures législatives prévoyant une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, elle ne s'opposait pas, dans des situations où un État membre faisait face à une menace grave pour la sécurité nationale qui s'avérait réelle et actuelle ou prévisible, à des mesures législatives permettant d'enjoindre aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace. Elle précisa qu'aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, les États membres pouvaient également prévoir – pour une période temporellement limitée au strict nécessaire – une conservation ciblée des données relatives au trafic et des données de localisation, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, ainsi que des adresses IP attribuées à la source d'une connexion Internet. Elle ajouta que les États membres pouvaient procéder à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, sans limite de temps.

241. Par ailleurs, elle jugea que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'opposait pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque le recours à ces techniques était limité à des situations dans lesquelles un État membre se trouvait confronté à une menace grave pour la sécurité nationale qui s'avérait réelle et actuelle ou prévisible, lorsque le recours à cette analyse pouvait faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision était dotée d'un effet contraignant, et lorsque le recours à un recueil en temps réel des données relatives au trafic et des données de localisation était limité aux personnes à l'égard desquelles il existait une raison valable de soupçonner qu'elles étaient impliquées dans des activités de terrorisme et qu'il était soumis à un contrôle préalable, effectué, soit par une juridiction,

soit par une entité administrative indépendante, dont la décision était dotée d'un effet contraignant.

IV. ÉLÉMENTS PERTINENTS DE DROIT ET PRATIQUE COMPARÉS

A. Les États contractants

242. Sept États au moins (l'Allemagne, la Finlande, la France, les Pays-Bas, le Royaume-Uni, la Suède et la Suisse) ont officiellement mis en place des régimes d'interception de communications en masse acheminées par câble et/ou voie aérienne.

243. Un projet de loi est cours de discussion dans autre État (la Norvège). Son adoption autoriserait l'interception de communications en masse.

244. Le régime mis en place en Suède est détaillé dans l'arrêt rendu dans l'affaire *Centrum för rättvisa c. Suède* (requête n° 35252/08). Les dispositions du régime en vigueur en Allemagne sont exposées aux paragraphes 247-252 ci-dessous.

245. S'agissant des accords de partage de renseignements, trente-neuf États membres au moins ont conclu de tels accords avec d'autres États ou prévoient la possibilité d'en conclure. Deux États membres s'interdisent expressément de demander à une puissance étrangère d'intercepter des éléments pour leur compte, deux autres s'autorisent expressément à recourir à cette pratique. La position des autres États sur cette question n'est pas claire.

246. Enfin, dans la plupart des États, les garanties en vigueur sont globalement identiques à celles qui s'appliquent aux opérations intérieures ; elles prévoient diverses limitations à l'utilisation des données obtenues et, dans certains cas, l'obligation de détruire les données en question lorsqu'elles ne présentent plus d'intérêt.

B. L'arrêt rendu par la Cour constitutionnelle fédérale allemande le 19 mai 2020 (1 BvR 2835/17)

247. Dans cette affaire, la Cour constitutionnelle fédérale allemande était appelée à statuer sur la question de savoir si les pouvoirs autorisant le Service fédéral du renseignement à mener des activités de renseignement stratégique (ou « renseignement d'origine électromagnétique ») sur les télécommunications passées par des étrangers se trouvant hors du territoire allemand étaient ou non contraires aux droits fondamentaux garantis par la Loi fondamentale (*Grundgesetz*).

248. Le régime de surveillance en cause portait sur l'interception du contenu des communications et des données de communication associées, et visait uniquement les télécommunications passées par des étrangers se

trouvant hors du territoire allemand. Il pouvait être mis en œuvre aux fins de l'acquisition de renseignements sur des sujets considérés par le gouvernement fédéral, dans le cadre de son mandat, comme étant importants pour la politique étrangère et de sécurité du pays, mais aussi pour cibler des personnes déterminées. La recevabilité et la nécessité des ordres d'interception décernés dans ce cadre étaient contrôlées par une commission indépendante. Il ressort de l'arrêt de la Cour constitutionnelle fédérale que les interceptions étaient suivies d'un processus entièrement automatisé de filtrage et d'évaluation en plusieurs étapes. À cette fin, le Service fédéral du renseignement utilisait des centaines de milliers de termes de recherche qui faisaient l'objet d'un contrôle par une sous-unité interne chargée de s'assurer que le lien entre les termes de recherche employés et le but de la demande d'informations était expliqué de manière raisonnable et détaillée. Après l'application du processus de filtrage automatisé, les données interceptées étaient effacées ou conservées et envoyées à un analyste pour évaluation.

249. Le partage d'éléments interceptés avec des services de renseignement étrangers était encadré par un accord de coopération qui devait comporter des restrictions d'utilisation et des garanties assurant que les données seraient traitées et effacées dans le respect de la légalité.

250. La Cour constitutionnelle a jugé que le régime en question n'était pas conforme à la Loi fondamentale. Tout en reconnaissant que la collecte efficace de renseignements étrangers répondait à un intérêt public impérieux, elle a néanmoins considéré, entre autres, que le régime incriminé n'était pas limité à des fins suffisamment spécifiques, qu'il n'était pas structuré de manière à permettre une supervision et un contrôle adéquats, et qu'il ne prévoyait pas certaines garanties, notamment à l'égard de la protection des journalistes, des avocats et d'autres personnes dont les communications devaient être spécialement protégées pour des raisons de confidentialité.

251. La Cour constitutionnelle a également jugé que les garanties applicables à l'échange de renseignements obtenus au moyen de la surveillance extérieure étaient insuffisantes. Elle a notamment observé que les situations dans lesquelles des intérêts importants étaient susceptibles de justifier des transferts de données n'étaient pas définies de manière suffisamment claire. En outre, tout en considérant qu'il n'était pas nécessaire que l'État destinataire dispose de règles comparables sur le traitement des données à caractère personnel, elle a néanmoins jugé que des données ne pouvaient être transférées à l'étranger que si celles-ci bénéficiaient d'un degré de protection adéquat et s'il n'y avait aucune raison de craindre que les informations transmises pourraient être utilisées pour porter atteinte aux principes fondamentaux de l'État de droit. Plus généralement, dans le contexte de l'échange de renseignements, elle a estimé que la coopération avec d'autres États ne devait pas être utilisée pour

affaiblir les garanties nationales et que, si le Service fédéral du renseignement souhaitait employer des termes de recherche qui lui avaient été fournis par des services de renseignement étrangers, il devait au préalable s'assurer que le lien nécessaire entre les termes de recherche et le but de la demande d'informations existait bien et que les données ainsi obtenues ne nécessitaient pas un degré particulier de confidentialité (par exemple parce qu'elles concernaient des donneurs d'alerte ou des dissidents). Bien qu'elle n'ait pas exclu la possibilité d'un transfert en masse de données à des services de renseignement étrangers, elle a jugé qu'il ne pouvait s'agir d'un processus continu fondé sur une seule finalité.

252. Enfin, la Cour constitutionnelle a constaté que les pouvoirs de surveillance en cause ne faisaient pas non plus l'objet d'un contrôle indépendant, étendu et continu propre à assurer le respect de la légalité et à compenser l'absence quasi-totale des garanties généralement reconnues dans un État de droit. Elle a indiqué qu'il incombait au législateur d'instaurer deux types de contrôle différents devant se refléter dans le cadre organisationnel, à savoir, d'une part, un contrôle assuré par une instance quasi-judiciaire ayant une fonction de supervision et le pouvoir de statuer selon une procédure formelle garantissant une protection juridique *a priori* ou *a posteriori* et, d'autre part, une supervision assurée par une instance administrative pouvant procéder de son propre chef à des contrôles aléatoires de l'ensemble des pratiques de surveillance stratégiques pour en vérifier la légalité. Elle a estimé que certaines phases cruciales de la procédure de surveillance devaient en principe être soumises à l'autorisation préalable d'une instance quasi-judiciaire, à savoir la définition exacte des diverses mesures de surveillance (sans exclure la possibilité de dérogations en cas d'urgence), l'utilisation de termes de recherche visant spécifiquement des personnes potentiellement dangereuses qui présentaient de ce fait un intérêt direct pour le Service fédéral du renseignement, l'utilisation de termes de recherche visant spécifiquement des personnes dont les communications devaient être spécialement protégées pour des raisons de confidentialité, et la transmission à des services de renseignement étrangers de données concernant des journalistes, des avocats et d'autres personnes dont les communications devaient être spécialement protégées pour des raisons de confidentialité.

C. L'arrêt rendu par la cour d'appel de La Haye le 14 mars 2017

253. Aux Pays-Bas, plusieurs personnes et associations reprochaient aux services de renseignement et de sécurité néerlandais de mener des opérations illicites consistant à recevoir des données émanant de services de renseignement et de sécurité étrangers tels que la NSA et le GCHQ qui, selon eux, obtenaient ou pouvaient avoir obtenu les données en question « sans autorisation » ou « illégalement ». Les plaignants ne soutenaient pas

que les activités de la NSA et du GCHQ étaient « illicites » ou « illégales » au regard du droit interne, mais ils avançaient que celles de la NSA enfreignaient le Pacte international relatif aux droits civils et politiques (« le PIDCP ») et que celles du GCHQ violaient la Convention. Ils s'appuyaient notamment sur les « révélations Snowden » (paragraphe 12 ci-dessus).

254. Les plaignants furent déboutés par le tribunal de La Haye le 23 juillet 2014 (ECLI:NL:RBDHA:2014:8966). L'appel qu'ils formèrent contre ce jugement fut rejeté par la cour d'appel de La Haye le 14 mars 2017 (ECLI:NL:GHDHA:2017:535).

255. Pour se prononcer ainsi, la cour d'appel estima qu'il fallait en principe faire confiance aux États-Unis et au Royaume-Uni pour se conformer à leurs obligations découlant des traités en question, et que cette présomption ne pouvait être renversée qu'en présence de circonstances suffisamment objectives pour que l'on pût considérer qu'elle ne se justifiait pas.

256. En ce qui concerne la collecte de données de télécommunications par la NSA, la cour d'appel conclut à l'absence d'indication claire de violation du PIDCP par cet organisme. Pour autant que les plaignants avançaient que les pouvoirs conférés aux autorités internes par la législation nationale en matière de collecte de données dépassaient les limites permises par le PIDCP, la cour d'appel considéra que les intéressés n'avaient pas suffisamment expliqué en quoi la loi et la réglementation pertinentes étaient inappropriées.

257. En ce qui concerne la collecte de données par le GCHQ, la cour d'appel jugea que les plaignants n'avaient apporté aucune preuve de leur allégation de violation de la Convention par cet organisme.

258. La Cour d'appel conclut en conséquence que les plaignants n'avaient pas démontré en quoi les activités de la NSA et du GCHQ contrevenaient, au moins dans leur principe, au PIDCP et à la Convention. Elle précisa que si l'on ne pouvait exclure qu'il soit arrivé à la NSA, au GCHQ ou à d'autres services de renseignement de collecter des données dans des conditions enfreignant le PIDCP ou la Convention, le principe de confiance s'opposait à ce que cette simple éventualité interdise aux services de renseignement néerlandais de recevoir des données de services de renseignement étrangers sans vérifier dans chaque cas que celles-ci avaient été obtenues dans le respect des obligations découlant des traités en question.

259. Enfin, la cour d'appel reconnut que même si les services de renseignement étrangers agissaient dans la limite des pouvoirs que leur conférait la loi et des obligations découlant des traités, le fait que ces pouvoirs puissent être plus étendus que ceux reconnus aux services de renseignement néerlandais pouvait être préoccupant dans certains cas, s'inquiétant par exemple de ce que les services de renseignement

néerlandais pourraient enfreindre la loi de 2002 sur les services de renseignement et de sécurité (ou l'esprit de ce texte) en obtenant de manière systématique ou délibérée auprès de services de renseignement étrangers des données relatives à des résidents des Pays-Bas, données que les pouvoirs qui leur sont reconnus ne leur permettent pas de recueillir. Elle releva que les restrictions imposées par la loi aux services de renseignement pourraient rester lettre morte dans cette hypothèse. Toutefois, elle constata que l'utilisation systématique ou délibérée de cette divergence entre le droit néerlandais et les droits étrangers par les services de renseignement néerlandais n'avait pas été établie ni démontrée par les plaignants.

260. Les plaignants saisirent la Cour suprême (*Hoge Raat*) d'un pourvoi en cassation dans lequel ils dénonçaient principalement les erreurs commises selon eux par la cour d'appel dans l'interprétation de leur grief et l'étendue de la charge de la preuve qui leur avait été imposée. Ils furent déboutés de leur pourvoi par un arrêt du 7 septembre 2018 (ECLI:NL:HR:2018:1434).

D. Les États-Unis d'Amérique

261. Les services de renseignement des États-Unis mènent le programme Upstream, dans les conditions prévues par l'article 702 de la FISA.

262. Le Procureur général et le Directeur du renseignement national délivrent chaque année des certificats autorisant le placement sous surveillance de personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis. Ils ne sont pas tenus de préciser à la FISC quelles personnes doivent être ciblées ni de démontrer qu'il existe des motifs raisonnables de penser que l'individu ciblé pourrait être un agent d'une puissance étrangère. En revanche, les certificats délivrés en application de l'article 702 indiquent les catégories d'informations à collecter, lesquelles doivent être conformes à la définition légale des informations de renseignement extérieur. Les certificats d'autorisation délivrés jusqu'à présent ont porté notamment sur le terrorisme international et l'acquisition d'armes de destruction massive.

263. Les certificats d'autorisation permettent à la NSA, avec l'aide que les fournisseurs de services sont tenus de lui fournir, de copier les flux de trafic Internet et d'y effectuer des recherches au fur et à mesure que les données circulent sur ce réseau. Tant les appels téléphoniques que les communications Internet sont collectés. Avant avril 2017, la NSA collectait des communications Internet « à destination » ou « en provenance » de sélecteurs ciblés, ou encore « en rapport » avec de tels sélecteurs. Une communication « à destination » ou « en provenance » d'un sélecteur était une communication dont l'expéditeur ou un destinataire était un utilisateur d'un sélecteur ciblé en vertu de l'article 702. Une communication « en

rapport » avec un sélecteur ciblé était une communication dans laquelle figurait ce sélecteur mais à laquelle la cible n'avait pas nécessairement participé. La collecte de communications « en rapport » avec un sélecteur impliquait donc des recherches sur le contenu des communications acheminées par Internet. Toutefois, la NSA a mis fin en avril 2017 à ses activités d'acquisition et de collecte de communications qui étaient simplement « en rapport » avec une cible. En outre, elle a déclaré que cette restriction de ses activités la conduirait à supprimer dès que possible la grande majorité des communications précédemment collectées sur Internet dans le cadre du programme Upstream.

264. L'article 702 de la FISA impose au gouvernement d'élaborer des procédures de ciblage et de minimisation qui font l'objet d'un contrôle par la FISC.

265. Le décret présidentiel n° 12333, signé en 1981, autorise la collecte, la conservation et la diffusion d'informations obtenues dans le cadre d'une enquête licite en matière de renseignement extérieur, de contre-espionnage, de trafic international de stupéfiants ou de terrorisme international. La surveillance de ressortissants étrangers autorisée par le décret présidentiel n° 12333 ne relève pas du champ d'application de la réglementation interne découlant de la FISA. On ignore quelle est la proportion des données collectées en vertu de ce décret par rapport à celles collectées en application de l'article 702.

EN DROIT

266. Les requérantes des trois affaires jointes estiment toutes que sont incompatibles avec les articles 8 et 10 de la Convention trois régimes de surveillance distincts, à savoir le régime d'interception en masse de communications instauré par l'article 8 § 4 de la loi de 2000 portant réglementation des pouvoirs d'enquête (*Regulation of Investigatory Powers Act 2000*, « la RIPA »), le régime de réception de renseignements provenant de services de renseignement étrangers et le régime d'acquisition de données de communication auprès de fournisseurs de services de communications.

267. Avant d'examiner séparément chacun de ces trois régimes, la Grande Chambre doit se prononcer sur une question préliminaire.

I. QUESTION PRÉLIMINAIRE DEVANT LA GRANDE CHAMBRE

268. Selon la jurisprudence constante de la Cour, « l'affaire » renvoyée devant la Grande Chambre englobe nécessairement tous les aspects de la requête telle qu'elle a été précédemment examinée par la chambre dans son arrêt. L'« affaire » renvoyée devant la Grande Chambre est la requête telle qu'elle a été déclarée recevable et comprend aussi les griefs qui n'ont pas

été déclarés irrecevables (voir *S.M. c. Croatie* [GC], nº 60561/14, § 216, 25 juin 2020, avec les références qui s'y trouvent citées).Selon la jurisprudence constante de la Cour, « l'affaire » renvoyée devant la Grande Chambre englobe nécessairement tous les aspects de la requête telle qu'elle a été précédemment examinée par la chambre dans son arrêt. L'« affaire » renvoyée devant la Grande Chambre est la requête telle qu'elle a été déclarée recevable et comprend aussi les griefs qui n'ont pas été déclarés irrecevables (voir *S.M. c. Croatie* [GC], nº 60561/14, § 216, 25 juin 2020, avec les références qui s'y trouvent citées).

269. En l'espèce, les requérantes ont introduit leurs requêtes en 2013, 2014 et 2015 respectivement. Leurs griefs portaient principalement sur les activités de surveillance menées en vertu de la RIPA et des codes de conduite s'y rapportant. Depuis lors, ces derniers ont été modifiés. Surtout, la loi de 2016 sur les pouvoirs d'enquête (« IPA ») a reçu la sanction royale le 29 novembre 2016, et ses dispositions ont commencé à entrer en vigueur en décembre 2016. Les nouveaux régimes de surveillance instaurés par ce texte sont dans une large mesure opérationnels depuis l'été 2018. Les dispositions du chapitre I de la partie I de la RIPA ont été abrogées en 2018.

270. La chambre a contrôlé la conformité à la Convention de la législation critiquée telle qu'elle était applicable à la date où elle a examiné la recevabilité des griefs des requérantes. Autrement dit, elle a examiné la législation telle qu'elle était en vigueur au 7 novembre 2017. Comme il s'agit là de la « requête telle qu'elle a été déclarée recevable », la Grande Chambre doit également limiter son examen à la législation en vigueur au 7 novembre 2017. Qui plus est, dès lors que les régimes juridiques progressivement instaurés à la suite de l'entrée en vigueur de l'IPA font actuellement l'objet de recours devant les juridictions internes, la Grande Chambre ne saurait examiner la nouvelle législation avant que celles-ci n'aient eu elles-mêmes l'occasion de le faire.

271. Les requérantes n'ayant pas contesté la conclusion de la chambre selon laquelle le Tribunal des pouvoirs d'enquête (*Investigatory Powers Tribunal* – « l'IPT ») offre désormais un recours effectif tant pour les griefs individuels que pour les griefs généraux portant sur la conformité à la Convention d'un régime de surveillance, et le Gouvernement n'ayant pas remis en cause sa conclusion selon laquelle les requérantes, compte tenu des circonstances de l'espèce, avaient épuisé les voies de recours internes au sens de l'article 35 § 1 de la Convention, il n'y a pas lieu, pour la Grande Chambre, d'examiner ces questions.

II. L'INTERCEPTION EN MASSE DE COMMUNICATIONS

A. Sur la compétence territoriale

272. En ce qui concerne le régime instauré par l'article 8 § 4 de la RIPA, le Gouvernement ne soulève pas d'exception sur le terrain de l'article 1 de la Convention et il n'argue pas que l'interception de communications échappait à la compétence territoriale du Royaume-Uni. En outre, au cours de l'audience qui s'est tenue devant la Grande Chambre, le Gouvernement a expressément confirmé qu'il ne soulèverait pas d'exception sur ce terrain, certaines au moins des requérantes relevant à l'évidence de la compétence territoriale de l'État. Dans ces conditions, aux fins de la présente affaire, la Cour partira du principe qu'en ce qui concerne les griefs des requérantes dirigés contre le régime instauré par l'article 8 § 4 de la RIPA, les faits dénoncés relevaient de la juridiction du Royaume-Uni.

B. Sur la violation alléguée de l'article 8 de la Convention

273. Les requérantes des trois affaires jointes estiment que le régime d'interception en masse de communications était incompatible avec l'article 8 de la Convention, ainsi libellé :

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, à la prospérité économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

1. L'arrêt de la chambre

274. La chambre a expressément reconnu que les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de système d'interception ils ont besoin pour protéger leur sécurité nationale, mais elle a estimé que la latitude qui leur est accordée pour la mise en œuvre de ce régime doit nécessairement être plus restreinte. À cet égard, elle a observé que la Cour a jugé que pour prévenir les abus de pouvoir, la loi doit énoncer les six « garanties minimales » suivantes : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées, la 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 les données interceptées peuvent

ou doivent être effacées ou détruites. Ces garanties, énoncées pour la première fois dans les affaires *Huvig c. France* (24 avril 1990, § 34, série A n° 176 B) et *Kruslin c. France* (24 avril 1990, § 35, série A n° 176-A), ont été régulièrement appliquées dans la jurisprudence de la Cour relative aux interceptions de communications, notamment dans deux affaires portant spécifiquement sur l'interception en masse de communications (*Weber et Saravia c. Allemagne* (déc.), n° 54934/00, CEDH 2006‑XI, et *Liberty et autres c. Royaume-Uni*, n° 58243/00, 1er juillet 2008).

275. La chambre a considéré que la décision d'utiliser un système d'interception en masse relève de la marge d'appréciation reconnue aux États. Elle a évalué le fonctionnement du régime d'interception en masse mis en œuvre au Royaume-Uni à l'aune des six garanties minimales mentionnées au paragraphe précédent. Les deux premières n'étant pas directement applicables à l'interception en masse, la chambre les a reformulées, recherchant d'abord si les motifs pour lesquels un mandat pouvait être émis étaient suffisamment clairs, ensuite si le droit interne fournissait aux citoyens des indications appropriées sur les circonstances dans lesquelles leurs communications étaient susceptibles d'être interceptées, et enfin s'il leur fournissait des indications appropriées sur les circonstances dans lesquelles leurs communications étaient susceptibles d'être sélectionnées pour examen. Par ailleurs, à la lumière de la jurisprudence récente (dont l'arrêt *Roman Zakharov c. Russie* [GC], n° 47143/06, CEDH 2015), la chambre a tenu compte également des modalités du contrôle de l'application des mesures de surveillance secrète, de l'existence d'un mécanisme de notification et des recours éventuellement prévus par le droit interne.

276. La chambre s'est déclarée préoccupée par les deux aspects suivants du régime instauré par l'article 8 § 4 de la RIPA, à savoir, premièrement, l'absence de supervision sur la sélection des canaux de transmission visés par les interceptions, sur les sélecteurs utilisés pour le filtrage des communications interceptées et sur le processus de sélection par les analystes des communications interceptées à examiner et, deuxièmement, l'absence de garanties réelles applicables à la recherche et à la sélection pour examen des données de communication associées. Compte tenu de la supervision indépendante exercée par le Commissaire à l'interception des communications et l'IPT, et des vastes enquêtes indépendantes consécutives aux révélations d'Edward Snowden, elle a estimé que le Royaume-Uni n'abusait pas de ses pouvoirs d'interception en masse. Néanmoins, au vu des lacunes susmentionnées, elle a conclu, à la majorité, que le régime d'interception en masse ne répondait pas à l'exigence de « qualité de la loi » et ne permettait pas de circonscrire l'« ingérence » au niveau « nécessaire dans une société démocratique ».

2. Thèses des parties

a) Les requérantes

277. Les requérantes soutiennent que dans son principe, l'interception en masse n'est ni nécessaire ni proportionnée au sens de l'article 8 de la Convention, et qu'elle ne relève donc pas de la marge d'appréciation accordée aux États. Elles estiment que l'arrêt rendu par la Cour dans l'affaire *Szabó et Vissy c. Hongrie* (n° 37138/14, 12 janvier 2016) donne à entendre que les mesures de surveillance secrète doivent être « strictement nécessaires » pour protéger les institutions démocratiques et obtenir des renseignements vitaux. Or elles considèrent qu'il n'est pas démontré que l'interception en masse satisfait à cette condition et que, si l'utilité de ce dispositif ne fait aucun doute, il ressort clairement de la jurisprudence de la Cour que tout ce qui est utile aux services de renseignement n'est pas nécessairement autorisé dans une société démocratique (*S. et Marper c. Royaume-Uni* [GC], nos 30562/04 et 30566/04, CEDH 2008).

278. Les requérantes avancent que l'interception d'une communication (de son contenu et/ou des données de communication associées), le stockage de celle-ci, son traitement automatisé et son analyse constituent autant d'ingérences distinctes dans le droit au respect de la vie privée et de la correspondance protégé par l'article 8. Elles admettent que l'examen d'une communication interceptée doit être qualifié d'ingérence « sérieuse », mais elles estiment qu'il est inexact de donner à entendre qu'il ne peut y avoir aucune ingérence significative avant ce stade. Selon elles, il ressort au contraire de la jurisprudence de la Cour que le simple fait de stocker des données à caractère personnel s'analyse en une grave ingérence dans les droits de l'individu garantis par l'article 8 de la Convention (voir, par exemple, *Rotaru c. Roumanie* [GC], n° 28341/95, CEDH 2000-V, et *S. et Marper*, précité), surtout lorsque ces données font l'objet d'un traitement automatisé. En effet, compte tenu de la progression rapide de la puissance de traitement et de l'apprentissage automatique, le stockage et le traitement électronique de données pourraient être en soi extrêmement intrusifs même lorsque personne n'examine le contenu de celles-ci ou les données de communication associées. À ce propos, et contrairement aux allégations du Gouvernement, les données collectées ne se présenteraient pas comme un « magma informe » (paragraphe 288 ci-dessous), mais plutôt comme un « catalogue méthodique et indexé permettant de trouver rapidement tout ce que l'on cherche ». Le traitement automatisé des données susciterait de sérieuses préoccupations quant au respect de la vie privée et, contrairement aux allégations du Gouvernement, ne réduirait pas les risques d'intrusion.

279. Par ailleurs, les requérantes soutiennent que si la Grande Chambre devait considérer que la mise en œuvre d'un régime d'interception en masse relève de la marge d'appréciation de l'État, force lui serait de conclure que

celui instauré par l'article 8 § 4 n'était pas prévu par la loi. À cet égard, elles avancent que, comme l'auraient constaté l'ensemble des contrôleurs indépendants, la RIPA était inutilement complexe, tant et si bien que la véritable nature et l'étendue de la surveillance mise en œuvre ne seraient clairement apparues qu'à la suite des révélations faites par Edward Snowden. En outre, les procédures « non publiques » auraient été arrêtées par le GCHQ lui-même, sans que le Parlement y ait eu accès et qu'il les ait approuvées. Elles auraient relevé de la politique interne et auraient donc pu être modifiées selon le bon vouloir de l'exécutif, et n'auraient eu aucun caractère contraignant. Dans ces conditions, elles ne devraient pas entrer en ligne de compte dans l'analyse de la Cour.

280. S'agissant de la prévisibilité du régime critiqué, les requérantes soutiennent que la Cour doit réviser son approche actuelle à l'aune de l'évolution de la société et de la technologie et renforcer les garanties requises afin de préserver le caractère concret et effectif des droits protégés par la Convention. Selon elles, la jurisprudence de la Cour en matière de surveillance massive est issue de la décision *Weber et Saravia* (précitée) rendue en 2006, c'est-à-dire à une époque bien différente de l'époque actuelle, où les smartphones étaient des appareils rudimentaires aux fonctionnalités limitées, où Facebook était utilisé principalement par des étudiants de l'Université et où Twitter venait d'être inventé. Aujourd'hui, les gens passeraient une grande partie de leur vie en ligne, utilisant Internet pour communiquer, diffuser des idées, effectuer des recherches, entretenir des relations, obtenir des conseils médicaux, tenir leurs journaux personnels, organiser leurs déplacements, écouter de la musique, s'orienter ou réaliser des opérations financières. En outre, la technologie moderne produirait des volumes considérables de données de communication, qui seraient très parlantes même en l'absence d'examen des données de contenu auxquelles elles sont associées, et qui seraient structurées de telle façon que les systèmes informatiques pourraient les traiter et y rechercher des constantes plus rapidement et efficacement qu'en appliquant un traitement analogue au contenu des communications elles-mêmes. Par exemple, les téléphones mobiles produiraient en permanence des données de communication en se connectant aux réseaux mobiles, ce qui permettrait d'enregistrer leur localisation, de suivre les déplacements de leurs utilisateurs et de savoir comment ceux-ci utilisent Internet.

281. Les requérantes estiment que l'autorisation judiciaire indépendante et préalable des mandats, du choix des sélecteurs et de la sélection des éléments interceptés doit figurer parmi les garanties révisées et renforcées dont elles réclament l'instauration. Elles considèrent en outre que pour que des sélecteurs ou des termes de recherche puissent viser un individu en particulier, il faudrait qu'il y ait des éléments objectifs justifiant un soupçon raisonnable à l'égard de celui-ci. Enfin, elles avancent que toute cible de surveillance clairement définie devrait être avisée *a posteriori* de la

surveillance dont elle a fait l'objet, lorsque cette information ne risque plus de porter gravement atteinte à l'intérêt public.

282. Selon les requérantes, le régime britannique d'interception en masse laissait à désirer à plusieurs égards. Premièrement, la mise en place d'une surveillance n'aurait pas été soumise à l'autorisation d'une instance indépendante, et moins encore à une autorisation judiciaire. Le fait qu'une autorisation judiciaire puisse ne pas constituer à elle seule une garantie suffisante contre les abus ne permettrait pas de conclure qu'elle n'est pas nécessaire. De plus, les sélecteurs et les termes de recherche utilisés par le GCHQ de renseignement auraient dû être soumis eux aussi à l'approbation d'une autorité, sinon judiciaire, du moins indépendante. Or ni les canaux de transmission visés par une interception ni les sélecteurs forts n'auraient été mentionnés dans les mandats d'interception.

283. Deuxièmement, la distinction entre les communications intérieures et les communications extérieures aurait été non seulement imprécise, mais encore dénuée de sens, la plupart des communications étant susceptibles de se trouver absorbées dans la catégorie des communications « extérieures ». De plus, il aurait été possible de mieux protéger les communications intérieures. Par exemple, en Suède, toutes les communications intérieures devraient être détruites dès leur découverte.

284. Troisièmement, les garanties applicables au contenu des communications des personnes dont on savait qu'elles se trouvaient dans les îles Britanniques auraient été limitées, et il n'y aurait eu pratiquement aucune garantie pour les données de communication associées. Le GCHQ aurait été en mesure de conserver l'intégralité des données de communication associées obtenues dans le cadre du régime d'interception en masse, sans autres limites que sa capacité de stockage et la durée de conservation maximale. Ces données, dont la collecte aurait revêtu un caractère extrêmement intrusif, auraient pu faire l'objet de recherches selon un facteur lié à un individu dont on savait qu'il se trouvait dans les îles Britanniques, sans qu'il soit nécessaire que le ministre certifie au préalable que la recherche était nécessaire et proportionnée au but visé.

285. Quatrièmement, les buts propres à justifier l'examen de communications n'auraient pas fait l'objet d'une définition juridique détaillée dans le régime critiqué, et la commission parlementaire aurait constaté que les certificats ministériels étaient formulés en termes « génériques ».

286. Enfin, les requérantes soutiennent que le Commissaire n'assurait qu'une supervision à temps partiel, avec des moyens limités, et qu'il était de ce fait dans l'incapacité d'exercer un contrôle efficace et rigoureux. Selon elles, l'efficacité de l'IPT était également limitée en ce que celui-ci ne pouvait remédier à l'absence d'autorisation judiciaire préalable et que les personnes qui s'adressaient à lui devaient de toute façon disposer

d'éléments donnant à penser qu'ils avaient fait l'objet d'une surveillance secrète pour qu'il puisse accueillir leurs plaintes.

b) Le Gouvernement

287. Le Gouvernement soutient que les informations obtenues au moyen du régime d'interception en masse litigieux revêtaient une importance cruciale pour la protection du Royaume-Uni contre les menaces pesant sur la sécurité nationale. Il affirme que ces renseignements lui ont permis non seulement de découvrir des menaces jusque-là inconnues, mais aussi de mettre sous surveillance des cibles connues se trouvant hors du ressort territorial du Royaume-Uni. Il expose que pour recueillir ne fût-ce qu'une petite partie des communications de cibles connues se trouvant à l'étranger, il faut intercepter toutes les communications passant par un ensemble de canaux de transmission sélectionnés, car les voies d'acheminement empruntées par les communications électroniques sont imprévisibles et celles-ci sont divisées en paquets pouvant être acheminés par des voies différentes. Il avance que l'interception en masse a été examinée en détail et à plusieurs reprises ces dernières années par différents organes indépendants, qui ont selon lui unanimement conclu qu'il n'existait « aucun autre moyen » (...) « ou combinaison de moyens suffisants pour se substituer à l'interception en masse ». Il considère qu'il est légitime d'accorder aux États une ample marge d'appréciation pour déterminer quels systèmes sont nécessaires à la protection de la collectivité contre ces menaces et que, lorsqu'elle exerce son contrôle sur ces systèmes, la Cour devrait se garder de porter atteinte à l'efficacité de dispositifs d'obtention de renseignements qui seraient susceptibles de sauver des vies et qui ne pourraient être recueillis par d'autres moyens.

288. Le Gouvernement avance que l'interception d'une communication dans le cadre du régime d'interception en masse ne constituait une ingérence significative dans les droits de la personne concernée garantis par l'article 8 que si cette communication avait été sélectionnée pour examen – c'est-à-dire incluse dans l'index de communications à partir duquel un analyste pouvait choisir des éléments à examiner – ou effectivement examinée par un analyste. Selon lui, l'atteinte portée aux droits de cette personne doit au contraire être considérée comme tout au plus minime lorsqu'une copie de sa communication avait été rejetée de manière quasi instantanée ou conservée quelques jours au maximum dans un « magma informe » de données, c'est-à-dire si elle avait fait l'objet d'une recherche par sélecteurs et requêtes, sans avoir été examinée ou utilisée. Dans leur écrasante majorité, les communications transitant par chacun des câbles sur lesquels les interceptions ont été réalisées n'auraient pas pu être « sélectionnées pour examen », et auraient donc dû être rejetées.

289. En ce qui concerne les garanties nécessaires, le Gouvernement considère, à l'instar de la chambre, qu'un régime d'interception en masse

doit être apprécié selon les normes découlant de la jurisprudence de la Cour relative à l'interception ciblée de communications. Il souscrit aussi en grande partie à l'appréciation du régime institué par l'article 8 § 4 de la RIPA à laquelle la chambre s'est livrée en s'appuyant sur les normes en question. Il réaffirme qu'une communication ne pouvait en aucun cas être consultée par un analyste tant qu'elle n'avait pas été sélectionnée pour examen à l'issue d'un processus de filtrage automatisé, que la sélection et l'examen pouvant en résulter étaient très soigneusement contrôlés, qu'aucun rapport de renseignement ne pouvait être établi sur une communication ou des données de communication sans qu'elles n'aient été consultées par un analyste, qu'en vertu de l'article 16 § 2 de la RIPA, le ministre devait certifier la nécessité et la proportionnalité de toute opération de recherche dans le contenu des communications selon un facteur lié à un individu dont on savait qu'il se trouvait dans les îles Britanniques, et que la supervision combinée de la commission parlementaire, du Commissaire et de l'IPT satisfaisait aux exigences découlant de la Convention. Selon lui, les garanties applicables à chacune des phases du processus d'interception en masse étaient fondées sur les principes de nécessité et de proportionnalité consacrés par la Convention. Ces principes fondamentaux se seraient appliqués d'abord à la collecte des données, puis à leur examen, à leur traitement, à leur stockage, à leur divulgation, à leur conservation et à leur suppression.

290. Le Gouvernement souhaite apporter des explications supplémentaires sur les aspects du régime dont la chambre a jugé qu'ils ne fournissaient pas de garanties adéquates contre les abus. En premier lieu, il reconnaît que les mandats ne mentionnaient pas quels étaient les canaux de transmission ciblés, mais il avance que l'inclusion de cette information dans les mandats se serait heurtée à des obstacles et à des difficultés considérables et que ceux-ci précisaient malgré tout les implications de l'interception et les catégories de canaux visés. Il ajoute que le GCHQ tenait le Commissaire à l'interception régulièrement informé de la base sur laquelle il sélectionnait les canaux de transmission à intercepter.

291. En deuxième lieu, le Gouvernement précise que le choix des sélecteurs était en réalité soigneusement contrôlé, indiquant qu'à chaque fois qu'un analyste ajoutait un nouveau sélecteur au système, il devait le mentionner par écrit en expliquant pourquoi l'application de ce sélecteur était nécessaire et proportionnée aux buts énoncés dans le certificat ministériel. Selon le Gouvernement, l'analyste réalisait cette opération en choisissant, dans un menu déroulant, un libellé auquel il ajoutait un texte libre expliquant pourquoi la recherche était nécessaire et proportionnée. Dans le cas d'un « sélecteur fort », l'analyste aurait dû préciser, par exemple, ce qui justifiait de rechercher les communications de telle ou telle cible, en quoi le sélecteur était pertinent par rapport aux modes de communication de la cible, et pourquoi la sélection des communications

concernées n'était pas susceptible d'entraîner une intrusion collatérale inacceptable dans la vie privée d'autres personnes. Dans le cas d'une nouvelle « requête complexe », l'analyste aurait dû concevoir les critères de sélection les plus susceptibles de permettre de repérer les communications renfermant des renseignements utiles, et il aurait dû expliquer là aussi en quoi ces critères étaient justifiés et pourquoi leur application était nécessaire et proportionnée aux buts indiqués dans le certificat ministériel. Les sélecteurs servant à la spécification ou à la découverte des cibles de surveillance auraient été utilisables trois mois au maximum avant qu'un contrôle ne s'impose.

292. Le Gouvernement expose que tout sélecteur devait être aussi spécifique que possible, afin de ne retenir que le minimum nécessaire à la réalisation des objectifs de la recherche de renseignements, et être proportionné au but visé. Il assure que s'il s'avérait, après analyse, qu'un sélecteur n'était pas utilisé par la cible qu'il visait, des mesures devaient être prises rapidement pour le retirer des systèmes concernés. Il ajoute que l'utilisation de sélecteurs devait être enregistrée dans un emplacement autorisé pour que ceux-ci puissent faire l'objet d'une vérification ultérieure et qu'un registre permettant de rechercher les sélecteurs utilisés devait être créé, afin que le Commissaire puisse exercer son contrôle. Il estime que ce dernier disposait ainsi des moyens nécessaires pour exercer un contrôle indépendant poussé des sélecteurs et des critères de recherche. Il avance qu'à l'époque de la publication de son rapport de 2014, le Commissaire avait justement mis en place des mécanismes et des processus pour s'assurer qu'il en allait bien ainsi et que, depuis l'arrêt de la chambre, les autorités gouvernementales s'efforcent, en collaboration avec le Commissariat, de renforcer la supervision des sélecteurs et des critères de recherche. Toutefois, il affirme qu'il est impossible de soumettre chaque sélecteur à une autorisation judiciaire préalable sans que sa capacité à détecter et à déjouer les menaces ne s'en trouve grandement altérée. Selon lui, les systèmes du GCHQ exploitent nécessairement des milliers de sélecteurs qui doivent parfois être promptement modifiés pour s'adapter aux évolutions rapides des investigations et des découvertes de menaces.

293. Le Gouvernement allègue que les communications auxquelles seul un « sélecteur fort » était appliqué étaient immédiatement écartées si elles n'y correspondaient pas. Il ajoute que les communications qui faisaient aussi l'objet d'une « requête complexe » étaient conservées quelques jours, le temps d'exécuter cette procédure, et qu'elles étaient ensuite effacées automatiquement, sauf si elles avaient été sélectionnées pour examen. Il expose que les communications sélectionnées pour examen ne pouvaient être conservées que tant que cette mesure était nécessaire et proportionnée et que, par défaut, la durée de conservation d'une communication sélectionnée ne pouvait dépasser quelques mois, après quoi celle-ci était automatiquement supprimée (étant précisé que les éventuels rapports de

renseignement mentionnant des éléments figurant dans la communication en question étaient conservés). Il aurait été possible, dans des cas exceptionnels, de solliciter par une demande motivée la prolongation de la durée de conservation de communications sélectionnées, dans les conditions fixées par le code de conduite en matière d'interception de communications.

294. Le Gouvernement réaffirme que tous les analystes appelés à examiner des éléments sélectionnés devaient y être spécialement autorisés, qu'ils suivaient régulièrement des formations obligatoires portant notamment sur les exigences de nécessité et de proportionnalité et qu'ils bénéficiaient d'une habilitation. Il indique qu'avant d'examiner des éléments, les analystes devaient rédiger une notice expliquant en quoi l'accès à ces éléments était nécessaire, conforme au certificat ministériel applicable et aux exigences de la RIPA, et proportionné au but visé (en tenant compte, le cas échéant, des circonstances susceptibles de donner lieu à une intrusion collatérale). Selon lui, les systèmes du GCHQ interdisaient l'accès aux éléments non accompagnés d'une telle notice.

295. En ce qui concerne les garanties applicables aux données de communication associées, le Gouvernement argue que l'examen du contenu des communications les plus sensibles et les plus privées implique toujours un degré d'intrusion plus élevé que l'examen de données de communication, même lorsque ces dernières sont agrégées pour déterminer précisément le lieu où se trouve un individu, les sites qu'il visite ou les personnes qu'il choisit de contacter. Selon lui, il faut donc que les règles qui régissent l'accès aux données de contenu demeurent plus exigeantes que celles qui régissent l'accès aux données de communication associées. Néanmoins, le ministre délivrant un mandat d'interception en masse devrait se voir imposer l'obligation de certifier la nécessité de l'examen des données de communication associées dans des conditions analogues (mais non identiques) à celles prévues par le régime de certification applicable au contenu des communications résultant de l'article 16 de la RIPA. Le nouveau code de conduite devrait être modifié en ce sens.

296. Cela dit, en attendant, le processus initial de filtrage appliqué aux données de communication aurait été identique à celui appliqué aux données de contenu, les systèmes de traitement du GCHQ écartant de manière automatique et quasi instantanée certains types de communications, tandis que les autres étaient ensuite soumises à des requêtes simples ou complexes par un traitement automatisé. Cependant, il y aurait eu deux grandes différences entre le traitement des données de contenu et celui des données de communication associées. D'abord, les garanties prévues à l'article 16 de la RIPA, qui exigeaient que des données relèvent d'un certificat ministériel pour pouvoir être examinées et qui interdisaient l'interception de données selon un facteur lié à un individu dont on savait qu'il se trouvait dans les îles Britanniques dans le but de retracer ses communications ne se seraient appliquées qu'aux données de contenu. Il aurait été matériellement

impossible d'appliquer cette garantie aux données de communication associées. Ces dernières auraient donné lieu à des requêtes beaucoup plus nombreuses (plusieurs milliers par semaine), et l'identité des personnes qu'elles concernaient aurait été dans bien des cas inconnue. De plus, ces données n'auraient eu bien souvent qu'une valeur temporaire, et s'il avait fallu attendre l'obtention d'un mandat spécifique pour y effectuer des recherches, leur utilité du point de vue du renseignement aurait pu s'en trouver sérieusement amoindrie. Il aurait été impossible d'exiger du ministre compétent qu'il certifie la nécessité et la proportionnalité dans chaque cas avant que des recherches puissent être entreprises.

297. Deuxièmement, les données de communication associées non sélectionnées pour examen n'auraient pas été immédiatement écartées, principalement parce qu'elles auraient surtout servi à découvrir des menaces ou des cibles ayant pu échapper au GCHQ dans un premier temps. Or la détection d'« inconnues inconnues » exigerait un travail d'analyse plus important, sur une longue période, qui supposerait très souvent l'agrégation de fragments de données de communication disparates en vue de la reconstitution d'un « puzzle » révélant une menace, opération qui nécessiterait parfois l'examen d'éléments à première vue dénués d'intérêt pour le renseignement. Ces tâches auraient été irréalisables si les données de communication non sélectionnées avaient dû être écartées immédiatement, ou au bout de quelques jours seulement.

298. Cela étant, le Gouvernement confirme que les analystes ne pouvaient examiner aucune donnée de communication sans avoir au préalable consigné les raisons pour lesquelles cet examen était nécessaire et proportionné à l'accomplissement des fonctions légales assignées au GCHQ. Cette exigence aurait conduit à la création de notices susceptibles de contrôle, où la justification de l'examen aurait figuré et qui auraient pu être vérifiées en cas d'inspection. De plus, aucun rapport de renseignement n'aurait pu être établi sur la base de données de communication non encore examinées. Enfin, les données de communication associées n'auraient pu être conservées que tant que cette mesure était nécessaire et proportionnée, pendant quelques mois au maximum, sauf si elles avaient fait l'objet d'une demande exceptionnelle de prolongation de la durée de conservation. En l'absence de pareille demande, elles auraient été automatiquement supprimées à l'expiration de leur durée maximale de conservation.

299. Enfin, eu égard à l'arrêt rendu par la chambre, le Gouvernement assure qu'il se prépare à prendre des mesures propres à garantir que la sélection pour examen de données – autres que des données de contenu – se rapportant à une personne dont on pense qu'elle se trouve dans les îles Britanniques donne lieu à la délivrance d'un certificat ministériel confirmant que cette opération est nécessaire et proportionnée au regard d'une base thématique précise. En attendant la mise en place d'un régime de certification « thématique » par voie de modification du code de conduite en

matière d'interception de communications découlant de la loi de 2016 sur les pouvoirs d'enquête, le GCHQ collaborerait avec le Commissariat pour élaborer un outil de gestion de l'information destiné à permettre au Commissaire de renforcer le contrôle *a posteriori* des données de communication associées. Le GCHQ aurait notamment modifié ses systèmes de façon à ce que chaque décision d'un analyste de sélectionner pour examen des données secondaires se rapportant à une personne dont on pense qu'elle se trouve dans les îles Britanniques par référence à un facteur lié à cette personne fasse l'objet d'un signalement accompagné des motifs justifiant la sélection des données en question.

3. Observations des tiers intervenants

a) Le gouvernement français

300. Le gouvernement français estime que face à des menaces telles que le terrorisme international et la criminalité transfrontalière, et au regard de la sophistication grandissante des technologies de communication, la surveillance stratégique de masse des communications revêt pour les États une importance déterminante pour la protection de la société démocratique. Selon lui, rien ne permet de dire qu'un système d'interception massive des communications est nécessairement plus intrusif qu'une interception ciblée puisque cette technique permet, par nature, d'obtenir et de traiter un plus grand nombre de communications concernant un individu donné. Par ailleurs, il n'y aurait aucune raison de considérer que les critères dégagés par la Cour dans la décision *Weber et Saravia* (précitée) ne sont pas tout aussi pertinents pour assurer un contrôle efficace de l'interception et du traitement de données réalisés dans le cadre d'un régime d'interception massive. Toutefois, les critères en question devraient être appliqués dans le cadre d'une appréciation globale comportant une mise en balance des éventuelles lacunes avec les garanties existantes et l'efficacité de la protection qu'elles offrent contre des abus éventuels.

301. Le gouvernement français soutient que rien ne justifie que soit ajouté à ces critères celui tiré de la nécessité d'un « soupçon raisonnable ». Il avance que les autorités ne sont en général pas en mesure de connaître par avance l'identité des personnes dont l'analyse des communications électroniques pourrait être utile dans l'intérêt de l'ordre public ou de la sécurité nationale, et qu'une telle exigence priverait cette mesure de surveillance de tout intérêt opérationnel. Selon lui, il n'est pas nécessaire qu'une autorité judiciaire intervienne pour autoriser la mise en œuvre d'une technique de renseignement, ni pour exercer un contrôle *a posteriori*, à condition que les organes en charge de cette autorisation et de ce contrôle soient, pour le premier d'entre eux, indépendant à l'égard de l'exécutif et, pour le second, investi de pouvoirs et attributions suffisants pour exercer un

contrôle efficace et permanent et que ces organes, enfin, soient indépendants l'un à l'égard de l'autre.

302. Enfin, le gouvernement français avance que la collecte de métadonnées est par nature moins intrusive que la collecte de données de contenu, les premières comportant selon lui moins d'informations sensibles sur le comportement et la vie privée de la personne concernée. Le rapport de la Commission de Venise (paragraphes 196-201 ci-dessus) et l'arrêt rendu par la CJUE dans l'affaire *Digital Rights Ireland* (paragraphes 209-213 ci-dessus) confirmeraient cette analyse.

b) Le gouvernement du Royaume des Pays-Bas

303. Le gouvernement néerlandais soutient lui aussi que l'interception en masse est nécessaire pour détecter des menaces inconnues contre la sécurité nationale. Il avance que les services de renseignement ont besoin d'instruments leur permettant d'enquêter promptement et efficacement sur les menaces nouvelles pour protéger la sécurité nationale. Selon lui, ces services doivent se voir conférer les pouvoirs nécessaires pour détecter et/ou déjouer non seulement les entreprises terroristes (telles que les projets d'attentat ainsi que les opérations de recrutement, de propagande et de financement), mais aussi les activités cybernétiques d'acteurs étatiques ou non-étatiques destinées à déstabiliser la démocratie (notamment en influençant des élections nationales ou en entravant des investigations poursuivies par des organisations nationales ou internationales, comme l'enquête menée à La Haye par l'Organisation pour l'interdiction des armes chimiques sur l'emploi d'armes chimiques en Syrie, qui aurait fait l'objet d'un tentative de piratage). En outre, la dépendance grandissante de secteurs vitaux (tels que la gestion des ressources hydriques, l'énergie, les télécommunications, le transport, la logistique, les ports et les aéroports) à l'égard des infrastructures numériques accroîtrait leur vulnérabilité aux cyberattaques. La désorganisation de ces secteurs aurait sur la société de très graves conséquences, beaucoup plus importantes que les pertes financières considérables qui en résulteraient.

304. De surcroît, le développement de nouveaux moyens de communication électronique et l'augmentation exponentielle du volume de données échangées et conservées à travers le monde compliqueraient encore la situation. Les interceptions ciblées seraient inefficaces car la nature et l'origine des menaces demeureraient dans bien des cas inconnues. Les interceptions en masse ne seraient pas aussi étroitement circonscrites que les interceptions ciblées, mais elles ne seraient jamais totalement aléatoires car elles viseraient des objectifs précis.

305. Par ailleurs, le gouvernement néerlandais estime que l'ajout de garanties minimales ou l'adaptation de celles qui existent déjà aux conditions actuelles ne s'impose pas, les garanties mises en place par la Cour étant à ses yeux suffisamment solides et durables. Il considère que les

critères supplémentaires que les requérantes ont invité la chambre à adopter – en particulier l'obligation de démontrer l'existence d'un soupçon raisonnable – réduiraient de manière inacceptable l'efficacité des services de renseignement sans renforcer réellement les droits fondamentaux des individus.

306. En outre, le gouvernement néerlandais estime que la distinction entre les données de contenu et les données de communication demeure pertinente, les premières étant selon lui vraisemblablement plus sensibles que les secondes. Il souscrit à l'avis de la chambre selon lequel il serait faux de présumer automatiquement que les interceptions en masse sont plus intrusives pour la vie privée que les interceptions ciblées puisque, du fait de leur nature même, ces dernières sont plus susceptibles d'aboutir à la collecte et à l'analyse d'un grand nombre de communications d'une même personne. Selon lui, tel n'est pas le cas des dispositifs d'interceptions en masse, dans lesquels les limites imposées à l'analyse et à l'utilisation des données circonscrivent le caractère intrusif de l'interception pour les droits fondamentaux des individus.

307. Enfin, le gouvernement néerlandais avance que compte tenu de la grande incertitude entourant l'origine des menaces, le fait d'imposer aux autorités une quelconque obligation d'expliquer ou de motiver dans les mandats le choix des sélecteurs ou des critères de recherche réduirait considérablement l'efficacité des interceptions en masse. Il soutient qu'un contrôle *a posteriori* constitue une garantie suffisante.

c) Le gouvernement du Royaume de Norvège

308. Le gouvernement norvégien plaide que les États doivent bénéficier d'une ample marge d'appréciation pour décider de la mise en place et des modalités de fonctionnement de dispositifs d'interception en masse pour les besoins de la sécurité nationale dès lors, selon lui, que les services de renseignement sont obligés de s'adapter aux évolutions rapides des technologies de l'information et de la communication. Les acteurs malveillants changeraient d'équipements et d'identité numériques si rapidement qu'ils deviendraient à la longue difficile à repérer. Il serait également difficile de détecter les cyberattaques et de les déjouer à temps sans outils capables de déceler les anomalies qu'elles entraînent et les traces qu'elles laissent. En conséquence, il serait indiscutablement nécessaire, pour les États, de se doter de moyens modernes, tels que l'interception en masse, pour déceler des menaces cachées dans le monde numérique et permettre aux services de renseignement de les détecter et de les surveiller.

309. Par ailleurs, le gouvernement norvégien estime que la Cour devrait exercer son contrôle en portant une appréciation globale sur le caractère adéquat et suffisant des garanties procédurales contre les abus et éviter d'imposer des exigences absolues. Il considère que la Cour devrait aussi se garder d'appliquer des critères ayant pour effet de porter indirectement

atteinte à l'ample marge d'appréciation dont les États doivent selon lui bénéficier pour utiliser un dispositif d'interception en masse dans l'intérêt de la sécurité nationale. Il avance que l'exigence d'un « soupçon raisonnable » ou d'une « notification *a posteriori* » aurait un tel effet.

310. Enfin, le gouvernement norvégien recommande à la Cour de ne pas transposer dans le système de la Convention les notions et critères utilisés par la CJUE. À cet égard, il avance, premièrement, qu'à l'époque pertinente dix-neuf États membres du Conseil de l'Europe n'étaient pas membres de l'Union européenne et, deuxièmement, que si la Convention et la Charte des droits fondamentaux ont de nombreux points communs, elles présentent cependant un certain nombre de différences, le second de ces instruments consacrant en particulier un droit à la protection des données personnelles dans son article 8. Il indique en outre que la CJUE a une conception différente de la « proportionnalité » en ce qu'elle applique un critère de « stricte nécessité » qui se distingue de celui utilisé par la Cour.

d) Le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression

311. Le rapporteur spécial avance que la surveillance jette une ombre sur les communications et qu'elle risque en conséquence de dissuader les individus de se livrer à des activités protégées par le droit international des droits de l'homme. Il ne faut pas en conclure, selon lui, que toutes les opérations de surveillance enfreignent les normes relatives aux droits de l'homme, certaines d'entre elles pouvant être acceptées à condition qu'elles satisfassent aux conditions de légalité, de légalité et de légitimité. Il estime toutefois que la comptabilité de toutes les formes d'activités de surveillance, avec les normes du droit international des droits de l'homme doit être strictement contrôlée.

312. Il considère que le droit à la vie privée doit être protégé non seulement en tant que droit fondamental autonome par rapport à tous les autres droits fondamentaux, mais aussi pour préserver d'autres droits, tels que la liberté d'opinion et d'expression, dont la jouissance suppose selon lui la reconnaissance d'une sphère d'intimité. Il rappelle avoir indiqué, dans son rapport de 2015, que les systèmes de surveillance peuvent compromettre le droit de se faire une opinion puisque la crainte de voir ses activités en ligne divulguées contre son gré dissuade d'accéder aux informations.

313. Il indique que la haut-commissaire des Nations unies a déconseillé dans un rapport de distinguer les métadonnées des données de contenu aux fins de l'appréciation de la gravité d'une ingérence dans les droits protégés par le Pacte international relatif aux droits civils et politiques (« le PIDCP »). Il précise que dans son rapport de 2014, la haut-commissaire a souligné que les agrégations de métadonnées réalisées par des autorités publiques pouvaient donner sur les individus davantage de détails d'ordre

privé que ceux que l'on obtiendrait en accédant au contenu de leurs communications privées. Il ajoute que la distinction entre les communications internes et les communications externes pourraient être contraires au PIDCP, que cet instrument impose aux États l'obligation de respecter et de garantir à toutes les personnes relevant de leur compétence l'ensemble des droits qu'il consacre, et que le Comité des droits de l'homme, dans la dernière en date de ses observations générales, a interprété cette obligation comme s'appliquant aux actes des États ayant sur ces droits des effets directs même en dehors de leurs territoires respectifs.

314. Enfin, le rapporteur spécial souligne l'importance des garanties contre d'éventuels abus, en particulier la nécessité d'un tribunal ou d'une autre instance décisionnelle pour contrôler l'application des mesures d'ingérence, la notification *a posteriori* des mesures de surveillance à ceux qu'elles visent, la publication d'informations sur l'étendue des méthodes et pouvoirs de surveillance, ainsi que le droit à un recours effectif en cas d'abus.

e) Access Now

315. Access Now avance que la surveillance massive en cause en l'espèce n'est pas conforme au PIDCP ni aux Principes internationaux sur l'application des droits de l'homme à la surveillance des communications, le Royaume-Uni n'ayant pas démontré que cette surveillance était strictement nécessaire et proportionnée au but visé. Elle ajoute que les programmes de surveillance ne doivent pas être envisagés de manière isolée, mais considérés dans le contexte de l'intégralité des activités de surveillance d'une nation, car l'apprentissage automatique (*machine learning*), par lequel des algorithmes mathématiques tirent des conclusions à partir d'ensembles de données, a accru le caractère invasif des mégadonnées (*big data*) et du forage de données (*data mining*).

f) Article 19

316. Article 19 soutient que la collecte, l'analyse et la conservation systématiques des communications de personnes sur lesquelles ne pèsent aucun soupçon sont en soi disproportionnées. Elle estime que seule une surveillance ciblée reposant sur des soupçons légitimes et autorisée par un juge peut éventuellement passer pour une restriction justifiée au droit à la vie privée.

g) European Digital Rights (« EDRi ») et d'autres associations de défense des droits de l'homme dans la société de l'information

317. EDRi et d'autres associations estiment que la présente affaire offre à la Cour une occasion cruciale de réviser son cadre de protection des métadonnées. Elles expliquent que les gouvernements ont construit leurs

programmes de surveillance en partant de la distinction établie entre contenu et métadonnées dans l'arrêt *Malone c. Royaume-Uni* (2 août 1984, série A n° 82), mais que lorsque cet arrêt a été rendu, ni Internet ni les téléphones mobiles n'existaient. Aujourd'hui, les métadonnées permettraient de brosser un portrait détaillé et intime d'une personne : elles permettraient de suivre son activité sur les réseaux sociaux, ses déplacements, ses navigations sur Internet ou encore ses habitudes de communication, et de savoir avec qui elle interagit. De plus, le niveau de détail pouvant être obtenu serait démultiplié par l'analyse sur une grande échelle. Ainsi, le directeur des services juridiques de la NSA, Stewart Baker, aurait indiqué que les métadonnées pouvaient tout révéler de la vie d'une personne, et que si l'on disposait de suffisamment de métadonnées, on n'avait pas besoin de données de contenu. Les associations concluent qu'il ne faut pas appliquer différents degrés de protection aux données personnelles en fonction de la distinction, selon elles arbitraire et dénuée de pertinence, entre contenu et métadonnées, mais en fonction des conclusions pouvant être tirées de ces données.

h) Open Society Justice Initiative (« OSJI »)

318. OSJI estime que le volume de données pouvant être interceptées de nos jours et l'appétit des gouvernements pour ces données sont de loin supérieurs à ce qui était envisageable par le passé, et que l'interception en masse constitue donc une ingérence particulièrement grave dans la vie privée, qui peut, par son « effet dissuasif », potentiellement porter atteinte à d'autres droits, tels que la liberté d'expression et la liberté d'association. Elle considère en conséquence que pour être licite, l'interception en masse doit respecter plusieurs conditions préalables : le cadre juridique doit être suffisamment précis, la collecte des informations doit être limitée dans le temps et dans l'espace, et elle ne doit avoir lieu qu'en présence d'un « soupçon raisonnable ».

i) La Fondation Helsinki pour les droits de l'homme (« la Fondation Helsinki »)

319. La Fondation Helsinki explique qu'elle a contesté la surveillance des communications opérée par les autorités publiques en Pologne, exposant que le Tribunal constitutionnel polonais a finalement jugé inconstitutionnels certains aspects de la législation pertinente, et que cette législation a ensuite été modifiée.

j) La Commission internationale de juristes

320. La Commission internationale de juristes avance que compte tenu de l'échelle et de l'ampleur de l'ingérence dans la vie privée résultant de la surveillance de masse, la distinction entre les métadonnées et les données de

contenu est une notion dépassée. Elle ajoute que le fait que, dans les opérations de surveillance de masse, l'ingérence dans les droits individuels puisse avoir lieu en partie dans une zone échappant à la compétence territoriale de l'État n'exclut pas la responsabilité de cet État, puisque celui-ci exerce sur les informations en question un contrôle suffisant pour que sa compétence se trouve établie.

k) The Law Society of England and Wales

321. The Law Society of England and Wales se déclare profondément préoccupée par les conséquences qui découlaient selon elle du régime prévu par l'article 8 § 4 de la RIPA sur le principe du secret professionnel des avocats. Ce régime aurait permis l'interception de communications protégées par la confidentialité et par le secret professionnel qu'échangent les avocats et leurs clients, même si les premiers comme les seconds se trouvaient au Royaume-Uni, ainsi que la collecte systématique des métadonnées correspondant à ces communications. De plus, une fois interceptées, ces communications couvertes par le secret professionnel des avocats auraient pu être utilisées dès lors que le mandat aurait eu pour objectif principal et pour objet la collecte de communications extérieures. Ce dispositif, combiné à l'absence de restrictions adéquates à l'utilisation de tels éléments, aurait été de nature à entraver considérablement la franchise et l'honnêteté des communications entre les avocats et leurs clients.

4. Appréciation de la Cour

a) Observations liminaires

322. Le présent grief porte sur l'interception en masse par les services de renseignement de communications transfrontières. Même si ce n'est pas la première fois que la Cour examine ce type de surveillance (*Weber et Saravia*, décision précitée, et *Liberty et autres*, arrêt précité), il est apparu au cours de la procédure que l'appréciation d'un tel régime soulève des difficultés spécifiques. À l'époque actuelle, où le numérique est de plus en plus présent, la grande majorité des communications se font sous forme numérique et sont acheminées à travers les réseaux mondiaux de télécommunication de manière à emprunter la combinaison de chemins la plus rapide et la moins chère sans aucun rapport significatif avec les frontières nationales. La surveillance qui ne vise pas directement les individus est par conséquent susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère. Il est donc essentiel autant que difficile de définir des garanties en la matière. Contrairement aux interceptions ciblées, qui sont l'objet d'une part importante de la jurisprudence de la Cour et qui sont avant tout utilisées dans le cadre d'enquêtes pénales, l'interception en masse est également – et peut-être essentiellement – utilisée pour recueillir des informations dans le

cadre du renseignement extérieur et pour détecter de nouvelles menaces provenant d'acteurs connus ou inconnus. Lorsqu'ils agissent dans ce domaine, les États contractants ont légitimement besoin d'opérer dans le secret, ce qui implique qu'ils ne rendent publiques que peu d'informations sur le fonctionnement du système, voire aucune ; en outre, les informations mises à la disposition du public peuvent être formulées en termes abscons et souvent largement différents d'un État à l'autre.

323. Si les capacités technologiques ont considérablement accru le volume des communications transitant par Internet au niveau mondial, les menaces auxquelles sont confrontés les États contractants et leurs citoyens ont également proliféré. On peut citer, sans être exhaustif, le terrorisme, le trafic de substances illicites, la traite des êtres humains ou encore l'exploitation sexuelle des enfants – activités d'échelle planétaire. Nombre de ces menaces proviennent de réseaux internationaux d'acteurs hostiles qui ont accès à une technologie de plus en plus sophistiquée grâce à laquelle ils peuvent communiquer sans être repérés. L'accès à cette technologie permet également à des acteurs étatiques ou non étatiques hostiles de perturber l'infrastructure numérique, voire le bon fonctionnement des processus démocratiques, au moyen de cyberattaques. Il y a là une menace grave pour la sécurité nationale qui, par définition, n'existe que dans le domaine numérique et ne peut donc être détectée et investiguée qu'à l'aide de moyens numériques. Ainsi, pour se prononcer sur la conformité à la Convention des régimes encadrant dans les États contractants l'interception en masse, technologie précieuse qui permet de détecter les nouvelles menaces de nature numérique, la Cour est appelée à examiner les garanties contre l'arbitraire et les abus qui y sont prévues tout en ne disposant que d'informations limitées sur la manière dont ils fonctionnent.

b) Sur l'existence d'une ingérence

324. Le Gouvernement ne conteste pas qu'il y ait eu ingérence dans les droits des requérantes garantis par l'article 8 de la Convention, mais il soutient que seule la sélection de communications pour examen a pu entraîner une ingérence significative dans les droits en question.

325. La Cour juge que l'interception en masse est un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance. Les régimes d'interception en masse ne sont pas forcément tous conçus exactement sur le même modèle, les différentes étapes du processus ne sont pas nécessairement distinctes et ne répondent pas toujours à un ordre chronologique strict. Sous réserve de ce qui précède, la Cour considère néanmoins que les étapes du processus d'interception en masse qu'il convient d'examiner peuvent être décrites comme suit :

(a) interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées) ;
(b) application de sélecteurs spécifiques aux communications retenues et aux données de communication associées ;
(c) examen par des analystes des communications sélectionnées et des données de communication associées ; et
(d) rétention subséquente des données et utilisation du « produit final », notamment partage de ces données avec des tiers.

326. Au cours de l'étape « (a) », les services de renseignement interceptent en masse des communications électroniques (ou des « paquets » de communications électroniques). Ces communications sont celles d'un grand nombre de personnes, dont la plupart ne présentent absolument aucun intérêt pour les services de renseignement. Certaines communications peu susceptibles de présenter un intérêt pour le renseignement peuvent être éliminées à ce stade.

327. La recherche initiale, qui est en grande partie automatisée, intervient lors de l'étape « (b) » : différents types de sélecteurs, y compris des « sélecteurs forts » (tels qu'une adresse de courrier électronique) et/ou des requêtes complexes, sont appliqués aux paquets de communications retenus et aux données de communication associées. À ce stade, il est possible que le processus commence à cibler des individus par l'utilisation de sélecteurs forts.

328. Lors de l'étape « (c) », les éléments interceptés sont examinés pour la première fois par un analyste.

329. Enfin, l'étape « (d) » est celle où les services de renseignement utilisent concrètement les éléments interceptés. Les éléments retenus peuvent alors être inclus dans un rapport de renseignement, communiqués à d'autres services de renseignement du pays, ou même transmis à des services de renseignement étrangers.

330. La Cour considère que l'article 8 s'applique à chacune des étapes décrites ci-dessus. Si l'interception suivie de l'élimination immédiate d'une partie des communications ne constitue pas une ingérence particulièrement importante, l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus d'interception en masse avance. À cet égard, la Cour a clairement dit que le simple fait de conserver des données relatives à la vie privée d'un individu s'analyse en une ingérence au sens de l'article 8 (*Leander c. Suède*, 26 mars 1987, § 48, série A n° 116), et que la nécessité de disposer de garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique (*S. et Marper*, précité, § 103). Le fait que les données retenues soient conservées sous une forme codée intelligible uniquement à l'aide de l'informatique et ne pouvant être interprétée que par un nombre restreint de personnes ne saurait avoir

d'incidence sur cette conclusion (voir *Amann c. Suisse* [GC], n° 27798/95, § 69, CEDH 2000-II, et *S. et Marper*, précité, §§ 67 et 75). En définitive, c'est à la fin du processus, lorsque des informations relatives à une personne en particulier sont analysées ou que le contenu de communications est examiné par un analyste, que la présence de garanties est plus que jamais nécessaire. Cette approche cadre avec les conclusions de la Commission de Venise qui, dans son rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique, a considéré que dans le processus d'interception en masse, les principales ingérences concernant la vie privée se produisent lorsque les autorités peuvent consulter les données conservées et les soumettre à un traitement (paragraphe 196 ci-dessus).

331. Ainsi, l'intensité de l'atteinte au droit au respect de la vie privée augmente au fur et à mesure que le processus franchit les différentes étapes. Afin de déterminer si cette ingérence croissante est justifiée, la Cour appréciera le régime institué par l'article 8 § 4 de la RIPA en se fondant sur cette analyse de la nature de l'ingérence en cause.

c) Sur le caractère justifié ou non de l'ingérence

i. Les principes généraux relatifs aux mesures secrètes de surveillance, y compris l'interception de communications

332. Une ingérence dans les droits garantis par l'article 8 ne peut se justifier au regard du paragraphe 2 de cet article que si elle est prévue par la loi, vise un ou plusieurs des buts légitimes énumérés dans ce paragraphe et est nécessaire, dans une société démocratique, pour atteindre ce ou ces buts (*Roman Zakharov*, précité, § 227 ; voir aussi *Kennedy c. Royaume-Uni*, n° 26839/05, § 130, 18 mai 2010). Les termes « prévue par la loi » signifient que la mesure litigieuse doit avoir une base en droit interne (et qu'il ne doit pas s'agir seulement d'une pratique ne reposant pas sur une base légale spécifique – voir *Heglas c. République tchèque*, n° 5935/02, § 74, 1er mars 2007). La mesure doit aussi être compatible avec la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8. La loi doit donc être accessible à la personne concernée et prévisible quant à ses effets (*Roman Zakharov*, précité, § 228 ; voir aussi, parmi bien d'autres, *Rotaru*, précité, § 52, *S. et Marper*, précité, § 95, et *Kennedy*, précité, § 151).

333. En matière de surveillance secrète, la « prévisibilité » ne peut se comprendre de la même façon que dans la plupart des autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la « prévisibilité » ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles de recourir à ce type de mesures de manière à ce qu'il puisse adapter sa conduite en conséquence. Cependant, le risque d'arbitraire

apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. En matière de mesures de surveillance secrète, il est donc indispensable qu'existent des règles claires et détaillées, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. Le droit interne doit être suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique est habilitée à recourir à pareilles mesures (*Roman Zakharov*, précité, § 229 ; voir aussi *Malone*, précité, § 67, *Leander*, précité, § 51, *Huvig*, précité, § 29, *Kruslin*, précité, § 30, *Valenzuela Contreras c. Espagne*, 30 juillet 1998, § 46, *Recueil des arrêts et décisions* 1998-V, *Rotaru*, précité, § 55, *Weber et Saravia*, décision précitée, § 93, et *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, n° 62540/00, § 75, 28 juin 2007). En outre, la loi doit définir l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire (*Roman Zakharov*, précité, § 230 ; voir aussi, entre autres, *Malone*, précité, § 68, *Leander*, précité, § 51, *Huvig*, précité, § 29, *Kruslin*, précité, § 30, et *Weber et Saravia*, décision précitée, § 94).

334. Dans les affaires où la législation autorisant la surveillance secrète est contestée devant la Cour, la question de la légalité de l'ingérence est étroitement liée à celle de savoir s'il a été satisfait au critère de la « nécessité », raison pour laquelle la Cour doit vérifier en même temps que la mesure était « prévue par la loi » et qu'elle était « nécessaire ». La « qualité de la loi » en ce sens implique que le droit national 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 (*Roman Zakharov*, précité, § 236, et *Kennedy*, précité, § 155).

335. À cet égard, il convient de rappeler qu'au fil de sa jurisprudence relative à l'interception de communications dans le cadre d'enquêtes pénales, la Cour a déterminé que pour prévenir les abus de pouvoir, la loi doit au minimum énoncer les éléments suivants : i) la nature des infractions susceptibles de donner lieu à un mandat d'interception ; ii) la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ; iii) la limite à la durée d'exécution de la mesure ; iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; v) les précautions à prendre pour la communication des données à d'autres parties ; et vi) les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites (*Huvig*, précité, § 34, *Kruslin*, précité, § 35, *Valenzuela Contreras*, précité, § 46, *Weber et Saravia*, décision précitée, § 95, et *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 76). Dans

l'arrêt *Roman Zakharov* (précité, § 231), elle a confirmé que ces mêmes garanties minimales, au nombre de six, s'appliquaient aussi dans les cas où l'interception était faite pour des raisons de sécurité nationale ; toutefois, pour déterminer si la loi litigieuse était contraire à l'article 8, elle a tenu compte également des éléments suivants : 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 (*Roman Zakharov*, précité, § 238).

336. Le contrôle et la supervision des mesures de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé. En ce qui concerne les deux premières phases, la Cour note que la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. Puisque la personne concernée sera donc nécessairement dans l'impossibilité d'introduire de son propre chef un recours effectif ou de prendre une part directe à quelque procédure de contrôle que ce soit, il est indispensable que les mécanismes existants procurent en eux-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le contrôle juridictionnel offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière (*Roman Zakharov*, précité, § 233 ; voir aussi *Klass et autres c. Allemagne*, 6 septembre 1978, §§ 55 et 56, série A n° 28).

337. Au troisième stade, c'est-à-dire lorsque la surveillance a cessé, la question de la notification *a posteriori* de mesures de surveillance est un élément pertinent pour apprécier l'effectivité des recours judiciaires et donc l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (*Roman Zakharov*, précité, § 234 ; voir aussi *Klass et autres*, précité, § 57, et *Weber et Saravia*, décision précitée, § 135) ou si – autre cas de figure – toute personne pensant avoir fait l'objet d'une surveillance a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de la surveillance n'a pas été informé des mesures prises (voir *Roman Zakharov*, précité, § 234 ; voir aussi *Kennedy*, précité, § 167).

338. Pour ce qui est de la question de savoir si une ingérence était « nécessaire dans une société démocratique » à la réalisation d'un but légitime, la Cour a reconnu que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder au mieux la sécurité nationale (*Weber et Saravia*, décision précitée, § 106).

339. Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent. La Cour doit se convaincre de l'existence de garanties adéquates et effectives contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale (ou tout autre intérêt national essentiel) risque de saper, voire de détruire, les processus démocratiques sous couvert de les défendre. L'appréciation de cette question est fonction de toutes les circonstances de la cause, telles que par exemple la nature, la portée et la durée des mesures pouvant être prises, 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. La Cour doit rechercher si les procédures de supervision de la décision et de la mise en œuvre de mesures restrictives sont de nature à circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique » (*Roman Zakharov*, précité, § 232 ; voir aussi *Klass et autres*, précité, §§ 49, 50 et 59, *Weber et Saravia*, décision précitée, § 106, et *Kennedy*, précité, §§ 153 et 154).

ii. Sur la nécessité de développer la jurisprudence

340. Dans la décision *Weber et Saravia* et dans l'arrêt *Liberty et autres* (tous deux précités), la Cour a admis que les régimes d'interception en masse n'étaient pas nécessairement exclus de la marge d'appréciation des États. Compte tenu, d'une part, de la prolifération des menaces que font aujourd'hui peser sur les États des réseaux d'acteurs internationaux qui utilisent Internet à la fois pour communiquer et comme outil et, d'autre part, de l'existence de technologies sophistiquées qui peuvent permettre à ces acteurs d'échapper à la détection (paragraphe 323 ci-dessus), elle considère que le recours à un régime d'interception en masse afin de repérer les menaces pesant sur la sécurité nationale ou sur des intérêts nationaux essentiels est une décision qui relève de cette marge d'appréciation.

341. Tant dans la décision *Weber et Saravia* que dans l'arrêt *Liberty et autres* (précités), la Cour a appliqué les six garanties minimales (mentionnées ci-dessus) énoncées dans sa jurisprudence relative aux interceptions ciblées (paragraphe 335 ci-dessus). Cependant, même si les régimes d'interception en masse qu'elle y a examinés étaient à première vue similaires à celui contesté dans le cas d'espèce, ces deux affaires remontent à plus de dix ans et, depuis, les progrès technologiques ont significativement modifié la manière dont on communique. On vit de plus en plus en ligne, ce qui génère un volume bien plus important de communications électroniques que celui qui pouvait être généré il y a dix ans, et les communications ont nettement évolué dans leur nature et leur qualité (paragraphe 322 ci-dessus). Par conséquent, l'étendue de l'activité de surveillance examinée dans ces deux affaires aurait été bien plus restreinte.

342. Il en va de même pour les données de communication associées. Comme indiqué dans le rapport établi à l'issue du contrôle des activités de

surveillance, pour chaque individu, le volume de données de communication actuellement disponible est normalement supérieur au volume de données de contenu, car chaque contenu s'accompagne de multiples données de communication (paragraphe 159 ci-dessus). Si le contenu d'une communication, crypté ou non, peut ne rien révéler d'utile sur son expéditeur ou son destinataire, les données de communication associées, en revanche, peuvent révéler un grand nombre d'informations personnelles telles que l'identité et la localisation de l'expéditeur et du destinataire, ou encore l'équipement par lequel la communication a été acheminée. De plus, toute intrusion occasionnée par l'acquisition de données de communication associées est démultipliée par l'interception en masse, car ces données peuvent désormais faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts (paragraphe 317 ci-dessus).

343. Un autre élément est plus important encore : dans la décision *Weber et Saravia* et dans l'arrêt *Liberty et autres* (tous deux précités), la Cour n'a pas expressément tenu compte du fait qu'il s'agissait d'une surveillance dont la nature et l'échelle étaient différentes de celles examinées dans les affaires précédentes. Or les interceptions ciblées et l'interception en masse présentent un certain nombre de différences importantes.

344. Pour commencer, l'interception en masse vise généralement les communications internationales (c'est-à-dire les communications qui traversent physiquement les frontières de l'État), et si l'on ne peut exclure que les communications de personnes qui se trouvent dans l'État qui opère la surveillance soient interceptées et même examinées, dans bien des cas le but déclaré de l'interception en masse est de contrôler des communications qui ne peuvent être contrôlées par d'autres formes de surveillance car elles sont échangées par des personnes se trouvant hors de la compétence territoriale de l'État. Le système allemand, par exemple, ne vise que le contrôle des télécommunications passées hors du territoire allemand (paragraphe 248 ci-dessus). En Suède, l'interception ne peut viser des données provenant de signaux échangés entre un expéditeur et un destinataire se trouvant tous deux sur le territoire suédois (voir l'arrêt rendu ce jour dans l'affaire *Centrum för rättvisa c. Suède* (requête n° 35252/08)).

345. Par ailleurs, comme cela a déjà été relevé, les buts dans lesquels on peut recourir à l'interception en masse sont en principe différents. Dans les affaires où la Cour a été amenée à examiner des interceptions ciblées, celles-ci étaient, pour la plupart d'entre elles, employées par les États défendeurs aux fins d'une enquête pénale. En revanche, si l'interception en masse peut elle aussi être employée pour enquêter sur certaines infractions

graves, les États membres du Conseil de l'Europe qui mettent en œuvre un régime d'interception en masse le font apparemment à des fins de collecte de renseignement extérieur, de détection précoce des cyberattaques et d'enquête sur celles-ci, de contre-espionnage et de lutte contre le terrorisme (paragraphes 303, 308 et 323 ci-dessus).

346. Si l'interception en masse n'est pas nécessairement utilisée pour cibler un individu en particulier, il est évident qu'elle peut être employée dans ce but – et qu'elle l'est. Lorsque c'est le cas, on ne surveille pas les appareils utilisés par les individus ciblés. On cible plutôt les individus par l'application de sélecteurs forts (tels que leur adresse de courrier électronique) aux communications interceptées en masse par les services de renseignement. Seuls les « paquets » de communications des individus ciblés qui sont passés par les canaux de transmission sélectionnés par les services de renseignement sont interceptés de cette manière, et seules les communications interceptées qui répondaient soit à un sélecteur fort soit à une requête complexe sont susceptibles d'être examinées par un analyste.

347. Comme tout système d'interception, l'interception en masse recèle à l'évidence un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée. Certes, l'article 8 de la Convention n'interdit pas de recourir à l'interception en masse afin de protéger la sécurité nationale ou d' autres intérêts nationaux essentiels contre des menaces extérieures graves, et les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet, cependant la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et un certain nombre de garanties doivent être mises en place. La Cour a déjà énoncé les garanties qui devraient caractériser un régime d'interceptions ciblées conforme à la Convention. Ces principes fournissent un cadre utile pour examiner la présente affaire, mais il y a lieu de les adapter pour prendre en compte les caractéristiques particulières de l'interception en masse et, en particulier, l'intensité croissante de l'ingérence dans l'exercice par l'individu de ses droits protégés par l'article 8 au fur et à mesure que l'opération passe par les étapes décrites au paragraphe 325 ci-dessus.

iii. L'approche à adopter dans les affaires relatives à l'interception en masse

348. À l'évidence, il n'est pas aisé d'appliquer à un régime d'interception en masse les deux premières des six « garanties minimales » (à savoir la nature des infractions susceptibles de donner lieu à un mandat d'interception et la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées, voir le paragraphe 335 ci-dessus), dont la Cour a dit, dans le contexte des interceptions ciblées, qu'elles devaient être clairement définies en droit interne pour prévenir les abus de pouvoir. De même, l'exigence d'un « soupçon raisonnable », que l'on trouve dans la jurisprudence de la Cour

relative aux interceptions ciblées pratiquées dans le cadre d'une enquête pénale, est moins pertinente dans le contexte des interceptions en masse, qui ont en principe un but préventif, que dans le contexte d'une enquête portant sur une cible précise et/ou une infraction identifiable. La Cour considère néanmoins qu'il est impératif que lorsqu'un État met en œuvre un tel système, le droit interne contienne des règles détaillées prévoyant les circonstances dans lesquelles les autorités peuvent avoir recours à de telles mesures. Le cadre juridique devrait, en particulier, énoncer avec suffisamment de clarté les motifs pour lesquels une interception en masse pourrait être autorisée et les circonstances dans lesquelles les communications d'un individu pourraient être interceptées. Les quatre autres garanties minimales définies par la Cour dans ses précédents arrêts – le droit interne doit définir la limite de la durée d'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 les données interceptées peuvent ou doivent être effacées ou détruites – sont quant à elles tout aussi pertinentes pour l'interception en masse.

349. Dans sa jurisprudence sur les interceptions ciblées, la Cour a tenu compte des dispositifs de supervision et de contrôle de l'application de mesures d'interception (*Roman Zakharov*, précité, §§ 233-234). Dans le contexte de l'interception en masse, la supervision et le contrôle des mesures revêtent une importance d'autant plus grande que le risque d'abus est inhérent à ce type d'interception et que le besoin légitime d'opérer dans le secret signifie inévitablement que, pour des raisons tenant à la sécurité nationale, les États ne sont souvent pas libres de divulguer des informations sur le fonctionnement du système en cause.

350. En conséquence, la Cour considère qu'afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus doit être encadré par des « garanties de bout en bout », c'est à dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*. Ces facteurs sont, de l'avis de la Cour, des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8 (voir aussi, dans le même sens, au paragraphe 197 ci-dessus, le rapport de la Commission de Venise, selon lequel deux des garanties les plus importantes dans un régime d'interception en masse sont l'autorisation et le contrôle du processus).

351. Pour ce qui est, tout d'abord, de l'autorisation, la Grande Chambre considère comme la chambre que si l'autorisation judiciaire constitue une

« importante garantie contre l'arbitraire », elle n'est pas une « exigence nécessaire » (voir les paragraphes 318 à 320 de l'arrêt de la chambre). L'interception en masse devrait néanmoins être autorisée par un organe indépendant, c'est-à-dire un organe indépendant du pouvoir exécutif.

352. Par ailleurs, afin de constituer une garantie effective contre les abus, l'organe indépendant chargé d'accorder les autorisations devrait être informé à la fois du but poursuivi par l'interception et des canaux de transmission ou des voies de communication susceptibles d'être interceptés. Cela lui permettrait d'apprécier la nécessité et la proportionnalité de l'opération d'interception en masse ainsi que de vérifier si la sélection des canaux est nécessaire et proportionnée aux buts dans lesquels les activités d'interception sont menées.

353. L'utilisation de sélecteurs – et en particulier de sélecteurs forts – est l'une des étapes les plus importantes du processus d'interception en masse puisqu'il s'agit du moment où les communications d'un individu déterminé sont susceptibles d'être ciblées par les services de renseignement. Toutefois, bien que certains régimes prévoient l'autorisation préalable des catégories de sélecteurs dont l'utilisation est envisagée (voir, par exemple, le régime en vigueur en Suède, décrit en détail dans l'arrêt *Centrum för rättvisa c. Suède* (requête n° 35252/08)), la Cour note que les gouvernements britannique et néerlandais ont soutenu que toute obligation d'expliquer ou de justifier les sélecteurs ou les critères de recherche dans l'autorisation restreindrait gravement l'effectivité de l'interception en masse (paragraphes 292 et 307 ci-dessus). L'IPT a retenu cet argument, jugeant que l'inclusion des sélecteurs dans l'autorisation aurait « inutilement compromis et limité la mise en œuvre des mandats tout en risquant de s'avérer illusoire » (paragraphe 49 ci-dessus).

354. Compte tenu des caractéristiques de l'interception en masse (paragraphes 344-345 ci-dessus), du grand nombre de sélecteurs et du besoin inhérent de flexibilité dans le choix des sélecteurs, qui peut en pratique s'exprimer par des combinaisons techniques de chiffres et de lettres, la Cour est disposée à admettre qu'inclure tous les sélecteurs dans l'autorisation ne serait probablement pas faisable en pratique. Toutefois, étant donné que le choix des sélecteurs et des termes de recherche détermine quelles sont les communications susceptibles d'être examinées par un analyste, l'autorisation devrait à tout le moins indiquer les types ou catégories de sélecteurs à utiliser.

355. Par ailleurs, des garanties renforcées devraient s'appliquer lorsque les services de renseignement emploient des sélecteurs forts se rapportant à des personnes identifiables. Les services de renseignement devraient être tenus de justifier – au regard des principes de nécessité et de proportionnalité – l'utilisation de chaque sélecteur fort, et cette justification devrait être consignée scrupuleusement et soumise à une procédure d'autorisation interne préalable comportant une vérification distincte et

objective de la conformité de la justification avancée aux principes susmentionnés.

356. Chaque stade du processus d'interception en masse – notamment l'autorisation initiale et ses éventuels renouvellements, la sélection des canaux de transmission, le choix et l'application de sélecteurs et de termes de recherche, l'utilisation, la conservation, la transmission à des tiers et la suppression des éléments interceptés – devrait également être soumis à la supervision d'une autorité indépendante, et cette supervision devrait être suffisamment solide pour circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique » (*Roman Zakharov*, précité, § 232 ; voir aussi *Klass et autres*, précité, §§ 49, 50 et 59, *Weber et Saravia*, décision précitée, § 106, et *Kennedy*, précité, §§ 153 et 154). L'organe de supervision devrait, en particulier, être en mesure d'apprécier la nécessité et la proportionnalité de la mesure prise, en tenant dûment compte du degré d'intrusion dans l'exercice par les personnes susceptibles d'être affectées de leurs droits protégés par la Convention. Afin de faciliter cette supervision, les services de renseignement devraient tenir des archives détaillées à chaque étape du processus.

357. Enfin, toute personne qui soupçonne que ses communications ont été interceptées par les services de renseignement devrait disposer d'un recours effectif permettant de contester la légalité de l'interception soupçonnée ou la conformité à la Convention du régime d'interception. Dans le contexte des interceptions ciblées, la Cour a considéré à plusieurs reprises que la notification ultérieure des mesures de surveillance était un facteur à prendre en compte pour apprécier le caractère effectif des recours judiciaires et donc l'existence de garanties effectives contre les abus des pouvoirs de surveillance. Elle a toutefois admis que la notification n'est pas nécessaire si le système de recours internes permet à toute personne soupçonnant que ses communications sont ou ont été interceptées de saisir les tribunaux, c'est-à-dire lorsque ceux-ci sont compétents même si l'intéressé n'a pas été informé de l'interception de ses communications (*Roman Zakharov*, précité, § 234, et *Kennedy*, précité, § 167).

358. La Cour considère qu'un recours qui ne dépend pas de la notification de l'interception à la personne concernée peut également constituer un recours effectif dans le contexte de l'interception en masse. Selon les circonstances, un tel recours pourrait même offrir de meilleures garanties de procédure régulière qu'un système fondé sur la notification. En effet, que les données aient été obtenues au moyen d'interceptions ciblées ou en masse, l'existence d'une exception de sécurité nationale pourrait priver l'obligation de notification de tout effet pratique réel. Il est plus probable qu'une obligation de notification ait peu d'effet pratique, voire en soit totalement dépourvue, dans le contexte de l'interception en masse, puisque pareille surveillance peut être utilisée dans le cadre d'activités de renseignement extérieur et cible, pour l'essentiel, les communications de

personnes ne relevant pas de la compétence territoriale de l'État. Ainsi, même si l'identité d'une cible est connue, les autorités peuvent ne pas connaître sa localisation.

359. Les pouvoirs dont dispose l'autorité et les garanties procédurales qu'elle offre sont des éléments à prendre en compte pour déterminer si le recours est effectif. Par conséquent, en l'absence de toute obligation de notification, il est impératif que le recours relève de la compétence d'un organe qui, sans être nécessairement judiciaire, soit indépendant de l'exécutif, assure l'équité de la procédure et offre, dans la mesure du possible, une procédure contradictoire. Les décisions de cet organe doivent être motivées et juridiquement contraignantes, notamment pour ce qui est d'ordonner la cessation d'une interception irrégulière et la destruction des éléments interceptés obtenus et/ou conservés de manière illégale (voir, *mutatis mutandis*, *Segerstedt-Wiberg et autres c. Suède*, n° 62332/00, § 120, CEDH 2006-VII, et *Leander*, précité, §§ 81-83, où l'absence de pouvoir de rendre une décision juridiquement contraignante représentait la principale faiblesse du contrôle offert).

360. Au vu de ce qui précède, la Cour devra, pour se prononcer sur la conformité à la Convention d'un régime d'interception en masse, en apprécier globalement le fonctionnement. À cet effet, elle recherchera principalement si le cadre juridique interne contient des garanties suffisantes contre les abus et si le processus est assujetti à des « garanties de bout en bout » (paragraphe 350 ci-dessus). Ce faisant, elle tiendra compte de la mise en œuvre effective du système d'interception, notamment des freins et contrepoids à l'exercice du pouvoir et de l'existence ou de l'absence de signes d'abus réels (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 92).

361. Pour déterminer si l'État défendeur a agi dans les limites de sa marge d'appréciation (paragraphe 347 ci-dessus), la Cour devra prendre en compte un groupe plus large de critères que les six garanties *Weber*. Plus précisément, en examinant conjointement les critères selon lesquels la mesure doit être « prévue par la loi » et « nécessaire », conformément à l'approche établie dans ce domaine (*Roman Zakharov*, précité, § 236, et *Kennedy*, précité, § 155), elle recherchera si le cadre juridique national définit clairement :

1. Les motifs pour lesquels l'interception en masse peut être autorisée ;
2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;
3. La procédure d'octroi d'une autorisation ;
4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;
5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;

6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;
7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;
8. Les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

362. Bien qu'il s'agisse de l'un des six critères *Weber*, la Cour n'a, à ce jour, fourni aucune indication spécifique concernant les précautions à prendre pour la communication d'éléments interceptés à d'autres parties. Or il est clair aujourd'hui que certains États partagent régulièrement des informations avec leurs partenaires du renseignement et, parfois même, leur donnent un accès direct à leur propre système. Dès lors, la Cour considère que la transmission, par un État contractant, d'informations obtenues au moyen d'une interception en masse à des États étrangers ou à des organisations internationales devrait être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et qu'elle devrait être soumise à certaines garanties supplémentaires relatives au transfert lui-même. Premièrement, les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne. Deuxièmement, l'État qui transfère les informations en question doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties. Cela ne signifie pas nécessairement qu'il doive garantir une protection comparable à celle de l'État qui transfère les informations, ni qu'une assurance doive être donnée avant chaque transfert. Troisièmement, des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles. Enfin, la Cour considère que le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant.

363. Pour les raisons exposées au paragraphe 342 ci-dessus, la Cour n'est pas convaincue que l'acquisition des données de communication associées dans le cadre d'une interception en masse soit nécessairement moins intrusive que l'acquisition du contenu des communications. Elle considère donc que l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications.

364. Cela étant, même si l'interception des données de communication associées est normalement autorisée en même temps que l'interception du contenu des communications, une fois qu'elles ont été obtenues, ces données peuvent faire l'objet d'un traitement différent par les services de renseignement (voir, par exemple, les paragraphes 153-154 ci-dessus). Compte tenu de la nature différente des données de communication associées et des différentes façons dont elles sont utilisées par les services de renseignement, la Cour est d'avis que, à condition que les garanties énoncées ci-dessus soient en place, il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications.

iv. Appréciation par la Cour du cas d'espèce

1) Observations préliminaires

365. À l'époque pertinente, l'interception en masse avait une base légale en droit interne, à savoir le chapitre I de la RIPA. En outre, la Cour estime que le régime qui en découlait avait pour buts légitimes la protection de la sécurité nationale, le maintien de l'ordre, la prévention des infractions et la protection des droits et libertés d'autrui. Dans ces conditions, et conformément à la méthodologie exposée au paragraphe 334 ci-dessus, il reste à rechercher si le droit interne était accessible et s'il offrait des garanties et des garde-fous effectifs et suffisants pour satisfaire aux exigences de « prévisibilité » et de « nécessité dans une société démocratique ».

366. Les dispositions législatives qui régissaient le fonctionnement du régime d'interception en masse étaient assurément complexes. De fait, la plupart des rapports établis sur les régimes de surveillance secrète mis en œuvre au Royaume-Uni ont critiqué leur manque de clarté (paragraphes 143, 152 et 157 ci-dessus). Toutefois, ces dispositions étaient clarifiées dans le code de conduite en matière d'interception de communications qui les complétait (paragraphe 96 ci-dessus). Le paragraphe 6.4 de ce code reconnaissait clairement l'existence d'opérations d'interception en masse et fournissait davantage de précisions sur le fonctionnement pratique de ce régime de surveillance (paragraphe 96 ci-dessus). Ce code était un document public approuvé par les deux chambres du Parlement et publié en ligne et en version imprimée par le gouvernement britannique. Tant les personnes exerçant des fonctions liées à l'interception de communications que les tribunaux devaient tenir compte de ses dispositions (paragraphes 93-94 ci-dessus). En conséquence, la Cour a admis que les dispositions en question pouvaient être prises en considération pour apprécier la prévisibilité de la RIPA (*Kennedy*, précité,

§ 157). Partant, elle reconnaît que le droit interne pertinent était suffisamment « accessible ».

367. En ce qui concerne le point de savoir si le droit interne contenait des garanties et des garde-fous effectifs et suffisants pour satisfaire aux exigences de « prévisibilité » et de « nécessité dans une société démocratique », la Cour examinera, dans la section β), l'interception du contenu de communications électroniques au regard de chacun des huit critères énumérés au paragraphe 361 ci-dessus. Dans la section γ), elle se penchera plus particulièrement sur l'interception des données de communication associées.

2) L'interception du contenu de communications

– *1. Les motifs pour lesquels une interception en masse de communications pouvait être autorisée*

368. L'article 5 § 3 de la RIPA et le paragraphe 6.11 du code de conduite en matière d'interception de communications (paragraphes 62 et 96 ci-dessus) disposaient que pour pouvoir émettre un mandat d'interception en masse, le ministre compétent devait s'assurer que cette mesure était nécessaire dans l'intérêt de la sécurité nationale, aux fins de la prévention ou de la détection des infractions graves ou aux fins de la sauvegarde de la prospérité économique du Royaume-Uni dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale.

369. Ces motifs étaient soumis à un certain nombre de limites. Premièrement, le Commissaire à l'interception des communications a précisé qu'en pratique, la protection de la « sécurité nationale » autorisait la surveillance d'activités menaçant la sécurité ou la prospérité de l'État ou visant à saper ou à renverser la démocratie parlementaire par des moyens politiques, par des actions collectives ou par la violence (*Kennedy*, précité, § 333). Deuxièmement, l'article 81 § 2 b) de la RIPA définissait l'infraction grave comme étant une infraction dont l'auteur (âgé d'au moins vingt et un an et sans antécédents judiciaires) pouvait raisonnablement s'attendre à être condamné à une peine d'emprisonnement d'une durée égale ou supérieure à trois ans, ou une infraction constituée par un acte caractérisé par l'usage de la violence, par un gain pécuniaire important ou par sa commission par une multiplicité de personnes poursuivant un objectif commun (paragraphe 63 ci-dessus). Troisièmement, l'article 17 de la RIPA et le paragraphe 8.3 du code de conduite en matière d'interception de communications prévoyaient qu'en règle générale, l'existence éventuelle d'une interception et les éléments interceptés eux-mêmes ne pouvaient jouer aucun rôle dans les procédures judiciaires (paragraphes 83 et 96 ci-dessus). Il s'ensuit que si l'interception pouvait servir à prévenir et à détecter les infractions graves, les éléments interceptés ne pouvaient être utilisés dans le cadre de poursuites pénales. En outre, le paragraphe 6.8 du code de conduite en matière d'interception de communications énonçait que le but d'un mandat

émis en vertu de l'article 8 § 4 la RIPA devait « en général correspondre à une ou plusieurs des priorités en matière de renseignement fixées par le Conseil de sécurité nationale » (paragraphes 96 et 98 ci-dessus).

370. En principe, plus les motifs sont étendus, plus le risque d'abus est important. Toutefois, le fait de restreindre les motifs et/ou de les définir plus étroitement ne peut constituer une garantie effective contre les abus que s'il existe d'autres garde-fous garantissant que l'interception en masse ne sera permise que pour des motifs autorisés et seulement si elle est nécessaire et proportionnée au but à atteindre. La question connexe de savoir s'il existe des garde-fous suffisants pour garantir que l'interception est nécessaire et justifiée est donc aussi importante que le degré de précision de la définition des motifs pour lesquels une interception peut être autorisée. En conséquence, la Cour estime qu'un régime qui autorise la mise en œuvre d'une interception pour des motifs relativement étendus peut néanmoins satisfaire aux exigences de l'article 8 de la Convention à condition que le système adopté comporte des garanties contre les abus qui, prises dans leur ensemble, soient suffisantes pour compenser cette déficience.

371. Si les motifs pour lesquels une interception en masse pouvait être autorisée au Royaume-Uni étaient formulés en termes relativement généraux, ils étaient axés sur la sécurité nationale ainsi que sur les infractions graves et la prospérité économique du Royaume-Uni dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale (paragraphe 368 ci-dessus). En conséquence, pour statuer sur la question de savoir si, pris dans son ensemble, ce régime satisfaisait aux exigences de l'article 8 de la Convention, la Cour doit à présent examiner les autres garanties prévues par le régime découlant de l'article 8 § 4.

– 2. Les circonstances dans lesquelles les communications d'un individu pouvaient être interceptées

372. Le paragraphe 6.2 du code de conduite en matière d'interception de communications (paragraphe 96 ci-dessus) énonçait clairement que « [c]ontrairement aux mandats relevant de l'article 8 § 1, les mandats relevant de l'article 8 § 4 ne [devaient] pas obligatoirement désigner nommément ou décrire le sujet de l'interception ou les lieux auxquels [devait] s'appliquer l'interception. L'article 8 § 4 n'impos[ait] pas non plus de limite expresse au nombre de communications extérieures pouvant être interceptées ». En d'autres termes, l'interception ciblait les canaux de transmission des communications, et non les appareils servant à envoyer les communications ou les expéditeurs ou destinataires de celles-ci. Le nombre de communications pouvant être interceptées n'étant pas limité, il semble que tous les paquets de communication acheminés par les canaux de transmission ciblés étaient interceptés pendant la durée de validité des mandats.

373. Cela étant, les mandats émis en vertu de l'article 8 § 4 étaient des mandats d'interception de communications extérieures (paragraphe 72 ci-dessus), et le paragraphe 6.7 du code de conduite en matière d'interception de communications (paragraphe 96 ci-dessus) imposait à l'agence interceptrice qui procédait à une interception dans le cadre de tels mandats d'utiliser sa connaissance de l'acheminement des communications internationales ainsi que des études régulières des différentes liaisons de communication pour identifier les canaux de transmission les plus susceptibles de contenir des communications extérieures répondant à la description des éléments mentionnés dans le certificat ministériel. L'agence interceptrice devait aussi intercepter les données de manière à limiter la collecte de communications non extérieures au minimum compatible avec le but assigné à l'interception des communications extérieures visées. Les canaux de transmission de communications n'étaient donc pas choisis au hasard, mais au contraire parce qu'ils étaient considérés comme étant les plus susceptibles d'acheminer des communications extérieures présentant un intérêt pour le renseignement.

374. Le paragraphe 6.5 du code de conduite en matière d'interception de communications définissait les « communications extérieures » comme étant celles envoyées ou reçues hors des îles Britanniques (paragraphe 96 ci-dessus). Les communications échangées entre un expéditeur et un destinataire se trouvant tous deux dans les îles Britanniques étaient en revanche des communications intérieures. La question de savoir si une communication était ou non « extérieure » dépendait donc du lieu où se trouvaient l'expéditeur et le destinataire de celle-ci, et non du chemin emprunté par elle pour arriver à destination. Les communications traversant les frontières du Royaume-Uni (les communications internationales) pouvaient cependant relever de la catégorie des communications « intérieures » puisqu'une communication (ou des paquets d'une communication) envoyée depuis le Royaume-Uni et reçue au Royaume-Uni pouvait avoir transité par un ou plusieurs autres pays.

375. La distinction entre les communications intérieures et les communications extérieures n'empêchait donc pas l'interception de communications intérieures ayant circulé à travers les frontières du Royaume-Uni. D'ailleurs, le fait que pareilles communications puissent se trouver accidentellement « prises dans les filets » d'une interception était expressément reconnu par l'article 5 § 6 de la RIPA, qui disposait que l'opération autorisée par un mandat d'interception couvrait l'interception de communications non indiquées dans le mandat si cette interception était nécessaire pour l'accomplissement d'actes que le mandat autorisait expressément (paragraphe 68 ci-dessus). En outre, la définition des communications « extérieures » était elle-même suffisamment large pour englober le stockage de données dans le « Cloud » ainsi que les activités de navigation sur Internet et d'utilisation des médias sociaux effectuées par une

personne se trouvant au Royaume-Uni (paragraphes 75 et 76 ci-dessus). Il n'en demeure pas moins, comme la chambre l'a reconnu, que la garantie limitant l'interception aux « communications extérieures » jouait un rôle au niveau macroscopique de la sélection des canaux de transmission sur lesquels les interceptions devaient être réalisées (voir le paragraphe 337 de l'arrêt de la chambre). Les agences interceptrices étant tenues d'utiliser leur connaissance de l'acheminement des communications internationales pour déterminer les canaux de transmission les plus susceptibles de contenir des communications extérieures utiles à l'opération envisagée, cette garantie restreignait – dans une mesure certes limitée – les catégories de personnes dont les communications étaient susceptibles d'être interceptées. Cette garantie était également pertinente en ce qui concerne la question de la proportionnalité, car les États pouvaient disposer de moyens moins intrusifs pour obtenir les communications des personnes relevant de leur compétence territoriale.

376. Au vu de ce qui précède, la Cour constate que le régime institué par l'article 8 § 4 de la RIPA autorisait manifestement l'interception de communications internationales (c'est-à-dire transfrontières) et que les services de renseignement ne devaient exercer leur pouvoir d'interception que sur les canaux de transmission les plus susceptibles d'acheminer des communications extérieures présentant un intérêt pour le renseignement. Dans le domaine de l'interception en masse, il est difficile d'imaginer, dans l'abstrait, comment il aurait été possible de circonscrire davantage les circonstances dans lesquelles les communications d'une personne étaient susceptibles d'être interceptées. En tout état de cause, dès lors que ni l'expéditeur ni le destinataire d'une communication électronique ne peuvent contrôler le chemin emprunté par celle-ci pour parvenir à destination, des restrictions supplémentaires à la sélection des canaux de transmission n'auraient en pratique pas rendu le droit interne plus prévisible quant à ses effets. En conséquence, la Cour admet que les circonstances dans lesquelles les communications d'une personne étaient susceptibles d'être interceptées en application du régime découlant de l'article 8 § 4 de la RIPA étaient suffisamment « prévisibles » aux fins de l'article 8 de la Convention.

– 3. La procédure d'octroi d'une autorisation

377. Les demandes de mandat relevant de l'article 8 § 4 de la RIPA devaient être adressées au ministre compétent, qui était seul habilité à délivrer des mandats de ce type. Avant d'être déposée, chaque demande faisait l'objet d'un contrôle au sein de l'agence dont elle émanait. Dans ce cadre, elle était examinée par plusieurs personnes, qui devaient vérifier si elle visait un but relevant de l'article 5 § 3 de la RIPA et si l'interception envisagée satisfaisait aux exigences de nécessité et de proportionnalité posées par la Convention (voir le paragraphe 6.9 du code de conduite en matière d'interception de communications, reproduit au paragraphe 96

ci-dessus). Si ce niveau supplémentaire de contrôle interne était incontestablement utile, il n'en demeure pas moins que les interceptions en masse réalisées à l'époque pertinente selon les modalités prévues par le régime découlant de l'article 8 § 4 de la RIPA étaient autorisées par le ministre compétent, et non par organe indépendant de l'exécutif. Dans ces conditions, force est de constater qu'il manquait au régime institué par l'article 8 § 4 de la RIPA une garantie fondamentale, à savoir la nécessité d'une autorisation indépendante et préalable des activités d'interception en masse (paragraphe 350 ci-dessus).

378. En ce qui concerne le degré de contrôle exercé par le ministre compétent, le paragraphe 6.10 du code de conduite en matière d'interception de communications énumérait de manière détaillée les informations qui devaient figurer dans les demandes de mandat (paragraphe 96 ci-dessus). Celles-ci devaient comporter une description des communications à intercepter, des informations relatives au(x) fournisseur(s) de services de communication, une évaluation de la faisabilité de l'opération – le cas échéant, une description de l'opération à autoriser, le certificat régissant l'examen des éléments interceptés (paragraphes 378 et 379 ci-dessous), un exposé des motifs pour lesquels l'interception était jugée nécessaire dans l'un ou plusieurs des buts énoncés à l'article 5 § 3 de la RIPA, un exposé des motifs pour lesquels l'opération que le mandat devait autoriser était proportionnée au but visé, l'assurance que les éléments interceptés ne seraient lus, consultés ou écoutés que dans la mesure où ils faisaient l'objet d'un certificat et répondaient aux conditions énoncées aux articles 16 § 2 à 16 § 6 de la RIPA et l'assurance que les éléments interceptés seraient traités dans le respect des garanties posées aux articles 15 et 16 de la RIPA.

379. Le ministre compétent était donc informé du but de l'opération (qui devait correspondre à l'un de ceux autorisés par l'article 5 § 3 de la RIPA) et il devait s'assurer, avant de délivrer un mandat, que cette mesure était nécessaire et proportionnée au but visé (voir les paragraphes 6.11 et 6.13 du code de conduite en matière d'interception de communications, reproduits au paragraphe 96 ci-dessus). Pour évaluer la proportionnalité de l'interception, le ministre devait vérifier si le mandat n'était pas excessif eu égard à l'ensemble des circonstances de l'espèce et s'il n'était pas raisonnablement possible d'obtenir par d'autres moyens moins intrusifs les informations recherchées (voir le paragraphe 3.6 du code de conduite en matière d'interception de communications, reproduit au paragraphe 96 ci-dessus). Pour ce faire, il devait mettre en balance l'ampleur et la portée de l'ingérence envisagée avec le but recherché, expliquer comment et pourquoi les méthodes à adopter causeraient l'intrusion la plus réduite possible pour le sujet et pour les tiers, rechercher, après examen de toutes les autres possibilités raisonnables, si la mesure envisagée constituait un moyen approprié d'obtenir le résultat nécessaire et préciser, autant qu'il était raisonnablement possible de le faire, quelles autres méthodes avaient

été envisagées et jugées insuffisantes pour parvenir aux objectifs opérationnels visés (voir le paragraphe 3.7 du code de conduite en matière d'interception de communications, reproduit au paragraphe 96 ci-dessus).

380. Les demandes de mandat relevant de l'article 8 § 4 de la RIPA devaient comporter « une description des communications à intercepter » ainsi que « des informations relatives au(x) fournisseur(s) de services de communication », mais le Gouvernement a confirmé à l'audience que les mandats ne précisaient pas quels étaient les canaux de transmission ciblés par l'interception, expliquant que pareille exigence se serait heurtée à de « sérieuses difficultés d'ordre pratique ». Il a toutefois indiqué que les implications de l'interception envisagée devaient faire l'objet d'une description appropriée, que les « catégories de canaux de transmission » ciblés devaient être précisées et que ces informations entraient en ligne de compte dans l'appréciation, par le ministre compétent, de la nécessité et de la proportionnalité des opérations mentionnées dans les demandes de mandat. En outre, il a confirmé, dans ses observations devant la Grande Chambre, que le GCHQ tenait le Commissaire à l'interception des communications régulièrement informé de la base sur laquelle il sélectionnait pour interception des canaux de transmission (paragraphe 290 ci-dessus).

381. La mention des catégories de sélecteurs à utiliser ne devait pas non plus obligatoirement figurer dans les demandes de mandat relevant de l'article 8 § 4 de la RIPA. Il n'était donc pas possible d'évaluer la nécessité et la proportionnalité des sélecteurs en question au stade de l'autorisation, mais le choix des sélecteurs faisait par la suite l'objet d'un contrôle indépendant. Dans ses observations devant la Grande Chambre, le Gouvernement a confirmé qu'à chaque fois qu'un analyste ajoutait un nouveau sélecteur au système, il devait le mentionner par écrit en expliquant pourquoi l'application de ce sélecteur était nécessaire et proportionnée aux buts énoncés dans le certificat ministériel, et qu'il réalisait cette opération en choisissant, dans un menu déroulant, un libellé auquel il ajoutait un texte libre expliquant pourquoi la recherche était nécessaire et proportionnée. En outre, le Gouvernement a précisé que l'utilisation de sélecteurs devait être enregistrée dans un emplacement autorisé pour que ceux-ci puissent faire l'objet d'une vérification ultérieure et qu'un registre permettant de rechercher les sélecteurs utilisés devait être créé, afin que le Commissaire à l'interception des communications puisse exercer son contrôle (paragraphes 291-292 ci-dessus). Le choix des sélecteurs était donc contrôlé par le Commissaire qui, dans son rapport annuel 2016, s'est déclaré « impressionné par la qualité » des explications relatives à la nécessité et à la proportionnalité des ajouts de sélecteurs formulées par les analystes (paragraphe 177 ci-dessus).

382. Le choix des sélecteurs et des termes de recherche déterminant les communications susceptibles d'être examinées par les analystes, la Cour a

indiqué qu'il est d'une importance fondamentale qu'au moins les catégories de sélecteurs soient identifiées dans l'autorisation et que l'utilisation de sélecteurs forts se rapportant à des personnes identifiables soit soumise à une autorisation interne préalable comportant une vérification séparée et objective de la conformité de la justification avancée aux principes susmentionnés (paragraphes 353-355 ci-dessus).

383. En l'espèce, l'absence de toute supervision de catégories de sélecteurs au stade de l'autorisation représentait une lacune du régime institué par l'article 8 § 4 de la RIPA. Le contrôle ultérieur de l'ensemble des sélecteurs individuels ne satisfaisait pas non plus à l'exigence d'un renforcement des garanties encadrant l'utilisation de sélecteurs forts liés à des individus identifiables et à la nécessité de mettre en place une procédure d'autorisation interne préalable comportant une vérification séparée et objective de la conformité de la justification avancée aux principes susmentionnés (paragraphe 355 ci-dessus). Si les analystes devaient enregistrer chacun des sélecteurs et justifier leur utilisation au regard des principes de nécessité et de proportionnalité posés par la Convention, et si les motifs justifiant cette utilisation étaient soumis à la supervision indépendante du Commissaire à l'interception des communications, il n'en demeure pas moins que les sélecteurs forts liés à des individus identifiables ne faisaient pas l'objet d'une autorisation interne préalable.

– 4. Les procédures à suivre pour la sélection, l'examen et l'utilisation d'éléments interceptés

384. Le paragraphe 6.4 du code de conduite en matière d'interception de communications disposait que lorsqu'un mandat émis en vertu de l'article 8 § 4 de la RIPA aboutissait à l'acquisition d'un gros volume de communications, les personnes autorisées de l'agence interceptrice pouvaient utiliser des sélecteurs forts et des recherches complexes pour générer un index (paragraphe 96 ci-dessus). Ce processus de sélection était encadré par l'article 16 § 2 de la RIPA et le paragraphe 7.19 du code de conduite en matière d'interception de communications, qui interdisaient l'utilisation d'un sélecteur lié à une personne dont on savait qu'elle se trouvait dans les îles Britanniques et ayant pour but la découverte d'éléments contenus dans les communications que cette personne envoyait ou qui lui étaient destinées, sauf si le ministre compétent avait personnellement autorisé l'emploi d'un tel sélecteur après s'être assuré que celui-ci était nécessaire dans l'intérêt de la sécurité nationale, aux fins de la prévention ou de la détection des infractions graves ou aux fins de la sauvegarde de la prospérité économique du Royaume-Uni – dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale – et qu'il était proportionné (paragraphes 85 et 96 ci-dessus).

385. Seuls les éléments figurant dans l'index pouvaient être consultés par un analyste (paragraphes 96 et 289 ci-dessus) et aucun rapport de

renseignement ne pouvait être établi sur une communication ou des données de communication sans qu'elles n'aient été consultées par un analyste (paragraphe 289 ci-dessus). En outre, le paragraphe 7.13 du code de conduite en matière d'interception de communications disposait que seuls les éléments décrits dans le certificat délivré par le ministre compétent pouvaient être examinés par un être humain, et qu'aucun agent ne pouvait accéder aux éléments interceptés autrement que dans la limite prévue par le certificat (paragraphe 96 ci-dessus). Par ailleurs, le paragraphe 6.4 prévoyait que pour pouvoir accéder à une communication, une personne autorisée de l'agence interceptrice devait au préalable expliquer pourquoi cet accès était nécessaire au regard de l'un des motifs énoncés dans le certificat accompagnant le mandat, et pourquoi l'accès constituait une mesure proportionnée dans le cas d'espèce, après avoir recherché s'il aurait été raisonnablement possible d'obtenir par d'autres moyens moins intrusifs les informations qu'elle visait à recueillir (paragraphe 96 ci-dessus).

386. Le certificat délivré par le ministre compétent en même temps que le mandat visait à garantir que les éléments interceptés feraient l'objet d'une sélection de manière à ce que seuls les éléments qu'il décrivait puissent être examinés par un être humain (voir les paragraphes 6.3 et 6.14 du code de conduite en matière d'interception de communications, reproduits au paragraphe 96 ci-dessus). Si les certificats jouaient un rôle important dans la réglementation de l'accès aux éléments interceptés, les rapports de la commission parlementaire sur le renseignement et du contrôleur indépendant de la législation sur le terrorisme ont critiqué le fait que les éléments mentionnés dans les certificats étaient désignés en termes très généraux (par exemple, « des éléments fournissant des renseignements sur le terrorisme (conformément à la définition figurant dans la loi de 2000 sur le terrorisme (version modifiée) ») (voir le paragraphe 342 de l'arrêt de la chambre et les paragraphes 146 et 155 ci-dessus). La Cour souscrit à la conclusion de la chambre selon laquelle il s'agissait là d'une lacune dans le système de garanties mis en place par le régime découlant de l'article 8 § 4 de la RIPA.

387. Toutefois, la commission parlementaire a observé que même si le certificat précisait les catégories générales d'informations susceptibles d'être examinées, c'étaient en pratique la sélection des canaux de transmission, l'application de sélecteurs simples et des critères de recherches initiaux, puis des recherches complexes, qui déterminaient quelles communications étaient examinées (paragraphes 146-147 ci-dessus). En d'autres termes, si les certificats encadraient la sélection, par les analystes, d'éléments figurant dans un index généré par ordinateur, c'était d'abord le choix des canaux de transmission et des sélecteurs et termes de recherche qui déterminait quelles étaient les communications susceptibles de figurer dans cet index (et qui pouvaient donc faire l'objet d'un examen). Or la Cour a déjà indiqué que l'absence d'identification des catégories de

sélecteurs dans les demandes de mandat et l'absence d'autorisation interne préalable des sélecteurs forts liés à un individu identifiable représentaient des lacunes du régime institué par l'article 8 § 4 de la RIPA (paragraphe 382 ci-dessus). Ces lacunes étaient aggravées par le caractère général des certificats ministériels. Non seulement il n'existait pas d'autorisation préalable indépendante des catégories de sélecteurs utilisés pour générer l'index et pas davantage d'autorisation interne ou indépendante des sélecteurs forts liés à un individu identifiable, mais les certificats régissant l'accès aux éléments figurant dans cet index n'étaient pas formulés de manière suffisamment précise pour fixer de véritables limites.

388. Le paragraphe 7.16 du code de conduite en matière d'interception de communications imposait aux analystes qui souhaitaient accéder à des éléments figurant dans l'index de mentionner au préalable les circonstances susceptibles de donner lieu à une atteinte collatérale à la vie privée, et toutes les mesures prises pour réduire l'ampleur de cette intrusion (paragraphe 96 ci-dessus). Par la suite, l'accès à ces éléments était accordé aux analystes pour une durée limitée, et si celle-ci était renouvelée, l'enregistrement correspondant devait être mis à jour avec les motifs du renouvellement (voir le paragraphe 7.17 du code de conduite, reproduit au paragraphe 96 ci-dessus). En vertu du paragraphe 7.18 du code de conduite, des audits devaient être réalisés périodiquement par des personnes chargées de s'assurer de la bonne tenue des enregistrements des demandes d'accès aux éléments et de vérifier que les éléments demandés relevaient des questions pour lesquelles le ministre compétent avait émis un certificat (paragraphe 96 ci-dessus).

389. En outre, le paragraphe 7.15 du code de conduite disposait que les éléments recueillis dans le cadre d'un mandat émis en vertu de l'article 8 § 4 de la RIPA ne pouvaient être lus, consultés ou écoutés que par des personnes autorisées (des analystes) qui suivaient régulièrement une formation obligatoire sur les dispositions de la RIPA ainsi que sur les exigences de nécessité et de proportionnalité, et qui disposaient du niveau d'habilitation adéquat (paragraphe 96 ci-dessus). En vertu du paragraphe 7.10, l'habilitation de chaque membre du personnel devait faire l'objet d'un réexamen périodique (paragraphe 96 ci-dessus).

390. Le paragraphe 7.6 du code de conduite disposait que les éléments interceptés ne pouvaient être copiés que dans la mesure nécessaire à la réalisation des buts autorisés et dans la stricte application du principe du « besoin d'en connaître », qui impliquait que seuls des extraits ou des résumés des éléments interceptés devaient être diffusés s'ils suffisaient à la personne qui avait besoin d'en avoir connaissance. L'article 15 § 5 de la RIPA imposait la mise en place de procédures garantissant que chaque copie d'éléments interceptés ou de données soit stockée de manière sécurisée pendant toute la durée de sa conservation (paragraphe 81 ci-dessus), et le paragraphe 7.7 du code de conduite exigeait en outre

qu'avant d'être détruits, les éléments interceptés et la totalité des copies, extraits et résumés qui en avaient été faits devaient être stockés de manière sécurisée, afin d'être inaccessibles aux personnes n'ayant pas le niveau d'habilitation requis (paragraphe 96 ci-dessus).

391. À l'exception des lacunes déjà signalées en ce qui concerne l'autorisation des sélecteurs (paragraphes 381 et 382 ci-dessus) et le caractère général des certificats ministériels (paragraphe 386 ci-dessus), la Cour estime que les conditions dans lesquelles des éléments interceptés pouvaient être sélectionnés, utilisés et conservés en vertu du régime découlant de l'article 8 § 4 de la RIPA étaient suffisamment « prévisibles » aux fins de l'article 8 de la Convention, et qu'elles offraient des garanties adéquates contre les abus.

– 5. Les précautions à prendre pour la communication d'éléments interceptés à d'autres parties

392. L'article 15 § 2 de la RIPA imposait de limiter au minimum nécessaire à la réalisation des « buts autorisés » le nombre de personnes auxquelles les éléments ou les données étaient divulgués ou accessibles, la mesure dans laquelle les éléments ou les données étaient divulgués ou accessibles, la mesure dans laquelle les éléments ou les données étaient copiés et le nombre de copies réalisées (paragraphe 78 ci-dessus). En vertu de l'article 15 § 4 de la RIPA et du paragraphe 7.2 du code de conduite, une chose était nécessaire pour les buts autorisés si et seulement si elle restait nécessaire ou était susceptible de le devenir pour les buts énumérés à l'article 5 § 3 de la RIPA, pour faciliter l'accomplissement de l'une quelconque des missions d'interception du ministre compétent, pour qu'une personne en charge de poursuites pénales dispose des informations dont elle avait besoin pour déterminer ce qu'elle était tenue de faire en vertu de son obligation d'assurer l'équité de la procédure (étant entendu que les éléments interceptés eux-mêmes ne pouvaient jouer aucun rôle dans la poursuite des infractions, voir le paragraphe 8.3 du code de conduite reproduit au paragraphe 96 ci-dessus) ou pour l'exécution de toute obligation imposée à toute personne par la législation relative aux archives publiques (paragraphes 80 et 96 ci-dessus).

393. Le paragraphe 7.3 du code de conduite interdisait la divulgation d'éléments interceptés à des personnes qui ne disposaient pas de l'habilitation requise et imposait l'application du principe du « besoin d'en connaître », selon lequel les éléments en question ne pouvaient être divulgués qu'aux personnes dont les fonctions se rattachaient à l'un des buts autorisés et qui avaient besoin d'en avoir connaissance pour accomplir ces fonctions. De même, les destinataires des éléments interceptés ne devaient en recevoir que la partie qu'ils avaient besoin de connaître (paragraphe 96 ci-dessus). Le paragraphe 7.3 s'appliquait aussi bien à la divulgation aux personnes appartenant à l'agence interceptrice qu'à la divulgation hors de

l'agence (paragraphe 96 ci-dessus). En vertu du paragraphe 7.4, les obligations énoncées au paragraphe 7.3 s'appliquaient non seulement à la personne qui avait intercepté les éléments mais aussi à toutes les personnes à qui ils étaient ensuite divulgués (paragraphe 96 ci-dessus).

394. Comme la chambre l'a observé, l'expression « susceptible de devenir nécessaire » n'ayant été définie ni dans la RIPA ni dans le code de conduite en matière d'interception de communications, ni d'ailleurs nulle part, l'article 15 § 4 de la RIPA et le paragraphe 7.2 du code auraient pu en pratique conférer aux autorités un large pouvoir de divulgation et de copie des éléments interceptés. Cependant, les éléments interceptés ne pouvaient de toute façon être divulgués qu'à une personne ayant le niveau d'habilitation requis et le « besoin d'en connaître », et seuls ceux que dont elle avait besoin de prendre connaissance pouvaient lui être communiqués. En conséquence, la Cour souscrit à la conclusion de la chambre selon laquelle l'expression « susceptible de devenir nécessaire » ne réduisait pas de manière significative les garanties protégeant les données obtenues au moyen d'une interception en masse (voir les paragraphes 368 et 369 de l'arrêt de la chambre).

395. S'agissant du transfert hors du Royaume-Uni d'éléments interceptés, la Cour considère que lorsque ces éléments avaient été interceptés conformément au droit interne, leur transmission à un service de renseignement étranger allié ou à une organisation internationale ne pouvait poser problème au regard de l'article 8 de la Convention que si l'État qui avait procédé à l'interception ne s'était pas assuré au préalable que son partenaire avait mis en place, pour le traitement de ces éléments interceptés, des garanties propres à prévenir tout abus ou ingérence disproportionnée et, en particulier, que celui-ci était en mesure de garantir la conservation sécurisée de ces éléments et de restreindre leur divulgation à d'autres parties (paragraphe 362 ci-dessus).

396. Il semble qu'au Royaume-Uni, les partenaires du réseau Five Eyes pouvaient accéder depuis leurs propres systèmes aux éléments obtenus en vertu des mandats d'interception délivrés au GCHQ (paragraphe 180 ci-dessus). En pareil cas, l'interception des éléments en question par les services de renseignement britanniques était censée avoir été réalisée conformément aux dispositions pertinentes droit interne, notamment l'article 8 § 4 de la RIPA pour ce qui importe en l'espèce. En vertu du paragraphe 7.5 du code de conduite en matière d'interception de communications, lorsque des éléments interceptés étaient divulgués à des autorités d'un pays ou territoire non britannique, les services de renseignement devaient prendre des mesures raisonnables pour s'assurer que ces autorités avaient mis en place et appliquaient les procédures nécessaires pour protéger les éléments interceptés et pour garantir qu'ils ne seraient divulgués, copiés, distribués et conservés que dans la stricte mesure du nécessaire. Les éléments interceptés ne pouvaient pas être de nouveau

divulgués aux autorités d'un autre pays ou territoire sans l'accord exprès de l'agence dont ils émanaient, et ils devaient être restitués à celle-ci ou détruits de manière sécurisée lorsqu'ils n'étaient plus nécessaires (paragraphe 96 ci-dessus). En outre, l'article 15 § 7 de la RIPA imposait la mise en place de restrictions empêchant que soit réalisée, dans le cadre d'une procédure menée hors du Royaume-Uni, une quelconque opération qui aurait abouti à la divulgation du contenu d'une communication ou des données de communication associées lorsque cette divulgation aurait été interdite au Royaume-Uni (paragraphe 82 ci-dessus).

397. En ce qui concerne les éléments confidentiels, le paragraphe 4.30 du code de conduite en matière d'interception de communications disposait que lorsque des informations confidentielles étaient transmises à un organe externe, des mesures raisonnables devaient être prises pour signaler leur caractère confidentiel, et qu'en cas de doute quant à la licéité de la transmission envisagée d'informations confidentielles, un conseiller juridique de l'agence interceptrice concernée devait être consulté avant la poursuite de la transmission (paragraphe 96 ci-dessus).

398. Force est donc de constater que des garanties avaient été mises en place pour assurer que les services de renseignement étrangers alliés veilleraient à conserver de manière sécurisée les éléments transmis et pour limiter leur divulgation à d'autres parties. La dernière garantie, à laquelle la Cour attache une importance particulière, résidait dans la supervision exercée par le Commissaire à l'interception des communications et l'IPT (paragraphes 411 et 414 ci-dessous).

399. Au vu de ce qui précède, la Cour estime que les précautions à prendre lors de la communication d'éléments interceptés à des tiers étaient suffisamment claires et offraient des garanties suffisamment solides contre les abus.

– *6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments devaient être effacés ou détruits*

400. En vertu de l'article 9 de la RIPA, les mandats émis sur le fondement de l'article 8 § 4 dans l'intérêt de la sécurité nationale ou pour la sauvegarde de la prospérité économique du Royaume-Uni – dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale – étaient valables six mois, mais ils pouvaient être renouvelés. La validité des mandats relevant de l'article 8 § 4 émis par le ministre compétent aux fins de la prévention des infractions graves était limitée à trois mois, sauf renouvellement. Ces mandats pouvaient être renouvelés à tout moment avant leur date d'expiration sur demande adressée au ministre, pour des durées de six et trois mois respectivement. La demande de renouvellement devait contenir les mêmes informations que la demande initiale, ainsi qu'une évaluation de l'utilité qu'avait eue l'interception jusqu'alors et un

exposé des raisons pour lesquelles elle restait nécessaire, au sens de l'article 5 § 3 de la RIPA, et proportionnée au but visé (voir l'article 9 de la RIPA, reproduit au paragraphe 67 ci-dessus, et les paragraphes 6.22 à 6.24 du code de conduite en matière d'interception de communications, reproduits au paragraphe 96 ci-dessus). Le ministre devait annuler les mandats – avant même leur date d'expiration initiale – s'il estimait que ceux-ci n'étaient plus nécessaires au regard de l'un des motifs énoncés à l'article 5 § 3 de la RIPA (voir l'article 9 de la RIPA, reproduit au paragraphe 67 ci-dessus).

401. Compte tenu des limites claires imposées à la durée des mandats émis en vertu de l'article 8 § 4 de la RIPA et de l'obligation faite aux autorités de les soumettre à une vérification permanente, la Cour considère que les règles relatives à la durée des interceptions prévues par le régime découlant de cet article étaient suffisamment claires et fournissaient des garanties adéquates contre les abus.

402. Le paragraphe 7.9 du code de conduite en matière d'interception de communications disposait que lorsqu'un service de renseignement recevait des éléments interceptés non analysés et les données de communication associées provenant d'une interception réalisée en application d'un mandat émis en vertu de l'article 8 § 4 de la RIPA, il devait fixer une durée maximale de conservation pour les différentes catégories d'éléments, en fonction de leur nature et du degré de l'intrusion dans la vie privée résultant de leur collecte. Les durées ainsi fixées ne devaient normalement pas dépasser deux ans, et elles devaient être convenues avec le Commissaire à l'interception des communications. Dans la mesure du possible, le respect des durées de conservation des éléments devait être assuré par un processus de suppression automatisée qui se déclenchait lorsque la durée maximale de conservation applicable aux éléments en question était atteinte (paragraphe 96 ci-dessus). Le paragraphe 7.8 du code de conduite imposait aux autorités de contrôler régulièrement les éléments interceptés conservés afin de vérifier que la raison justifiant leur conservation demeurait valable au regard de l'article 15 § 3 de la RIPA (paragraphe 96 ci-dessus).

403. Dans ses observations devant la Grande Chambre, le Gouvernement a apporté des explications complémentaires au sujet des durées de conservation. Il a indiqué que les communications auxquelles seul un « sélecteur fort » était appliqué étaient immédiatement écartées si elle n'y correspondaient pas, que les communications qui faisaient aussi l'objet d'une « requête complexe » étaient conservées quelques jours, le temps d'exécuter cette procédure, et qu'elles étaient ensuite effacées automatiquement, sauf si elles avaient été sélectionnées pour examen, et que les communications sélectionnées pour examen ne pouvaient être conservées que tant que cette mesure était nécessaire et proportionnée. Il a expliqué que par défaut, la durée de conservation d'une communication sélectionnée ne pouvait dépasser quelques mois, après quoi celle-ci était

automatiquement supprimée (étant précisé que les éventuels rapports de renseignement mentionnant des éléments figurant dans la communication en question étaient conservés), mais qu'il était possible, dans des cas exceptionnels, de solliciter par une demande motivée la prolongation de la durée de conservation (paragraphe 293 ci-dessus). Il ressort de ces explications que les durées de conservation étaient en pratique nettement plus courtes que la durée maximale autorisée, à savoir deux ans.

404. Enfin, l'article 15 § 3 de la RIPA et le paragraphe 7.8 du code de conduite en matière d'interception de communications exigeaient que la totalité des copies, extraits et résumés d'éléments interceptés soient détruits de manière sécurisée dès que leur conservation n'était plus nécessaire à la réalisation d'un but énoncé à l'article 5 § 3 (paragraphes 79 et 96 ci-dessus).

405. Dans l'affaire *Liberty*, l'IPT a examiné les procédures qui régissaient la conservation des éléments et leur destruction, et les a jugées adéquates (paragraphe 50 ci-dessus). La Cour considère elle aussi que les procédures « publiques » qui fixaient les conditions dans lesquelles les éléments interceptés devaient être effacés ou détruits étaient suffisamment claires. Elle estime toutefois qu'il aurait été souhaitable que les durées de conservation plus courtes indiquées par le Gouvernement au cours de la présente procédure soient reflétées dans des dispositions législatives et/ou d'autres mesures d'ordre général.

– *7. La supervision*

406. La supervision du régime découlant de l'article 8 § 4 de la RIPA relevait au premier chef de la responsabilité du Commissaire à l'interception des communications, quoique celui-ci ait souligné « le rôle capital de contrôle de la qualité exercé en amont par le personnel et les juristes de l'agence interceptrice ou du service de délivrance des mandats » qui fournissaient au ministre compétent des conseils indépendants et effectuaient un important travail d'analyse préalable des demandes de mandats et des demandes de renouvellement pour veiller à ce que les mesures sollicitées soient (et demeurent) nécessaires et proportionnées au but visé (paragraphe 170 ci-dessus).

407. Le Commissaire à l'interception des communications était indépendant de l'exécutif et du législateur, et devait exercer ou avoir exercé de hautes fonctions judiciaires. Il avait pour principale mission de contrôler la mise en œuvre, par les ministres et les pouvoirs publics concernés, des pouvoirs découlant de la partie I – et, dans une moindre mesure, de la partie III – de la RIPA et de diriger un mécanisme d'inspection qui lui permettait de superviser de manière indépendante la manière dont la loi était appliquée. Il rendait régulièrement compte de ses activités au Premier ministre sur une base semestrielle, et préparait un rapport annuel remis aux deux chambres du Parlement. En outre, à l'issue de chaque inspection, un rapport contenant des recommandations officielles était adressé au chef de

l'autorité publique concernée, laquelle était tenue de confirmer dans un délai de deux mois que ces recommandations avaient été mises en œuvre ou de rendre compte des progrès accomplis. Les rapports périodiques du Commissaire à l'interception des communications ont été publiés à partir de 2002, et dans leur intégralité – sans annexes confidentielles – à partir de 2013. En outre, l'article 58 § 1 de la RIPA imposait à tous les fonctionnaires appartenant aux services qui relevaient de la compétence du Commissaire de lui présenter ou de lui remettre tous les documents ou informations qui pouvaient s'avérer nécessaires pour l'exercice de ses fonctions (paragraphes 135 et 136 ci-dessus).

408. Le rapport annuel 2016 du Commissaire témoigne de l'ampleur des pouvoirs de supervision exercés par celui-ci. En résumé, au cours de ses inspections, le Commissaire a évalué les systèmes mis en place pour l'interception de communications en s'assurant que toutes les informations pertinentes avaient été enregistrées, il a examiné plusieurs demandes d'interception afin de vérifier qu'elles étaient nécessaires et qu'elles répondaient aux exigences de nécessité et de proportionnalité, il s'est entretenu avec des agents chargés du traitement des affaires et avec des analystes afin de déterminer si les interceptions et la justification de l'acquisition des éléments interceptés répondaient aux exigences de proportionnalité, il a examiné les éventuelles approbations orales urgentes, afin de vérifier que le recours à la procédure d'urgence avait été justifié et approprié, il a contrôlé les cas d'interception et de conservation de communications protégées par le secret professionnel ou la confidentialité, ainsi que tous les cas où un avocat avait fait l'objet d'une enquête, il a vérifié que les garanties et procédures mises en place en vertu des articles 15 et 16 de la RIPA étaient adéquates, il a étudié les procédures mises en place pour la conservation, le stockage et la destruction des éléments interceptés et des données de communication associées et il a analysé les erreurs signalées, vérifiant que les mesures instaurées pour empêcher que ces erreurs ne se reproduisent étaient suffisantes (paragraphe 171 ci-dessus).

409. En 2016, le commissariat a inspecté les neuf agences interceptrices une fois et les quatre principaux services de délivrance de mandats deux fois. Au cours de ces inspections, 970 mandats ont été examinés, soit 61 % du nombre de mandats en vigueur à la fin de l'année et 32 % du total des nouveaux mandats émis en 2016 (paragraphes 173 et 175 ci-dessus).

410. Les inspections se déroulaient normalement en trois étapes. D'abord, pour disposer d'un échantillon représentatif de mandats, les inspecteurs sélectionnaient des mandats visant différents types d'infractions et différents types de menaces pour la sécurité nationale, en recherchant en priorité des mandats d'un intérêt particulier ou particulièrement sensibles. Ensuite, au cours des jours d'analyse qui précédaient les inspections, ils examinaient en détail les mandats sélectionnés et les documents associés. À

ce stade, les inspecteurs pouvaient contrôler les déclarations relatives à la nécessité et à la proportionnalité de l'accès aux données formulées par les analystes lors de l'ajout de sélecteurs au système de collecte de données pour examen. Chaque déclaration devait se suffire à elle-même et répondre à l'exigence générale de respect des priorités en matière de collecte de renseignement. Enfin, les inspecteurs identifiaient les mandats, opérations ou parties de la procédure appelant des informations ou des précisions complémentaires, et ils organisaient un entretien avec le personnel opérationnel, juridique ou technique concerné. Si nécessaire, ils examinaient plus avant la documentation ou les systèmes concernant ces mandats (paragraphe 174 ci-dessus).

411. Le Commissaire à l'interception des communications supervisait aussi l'échange d'éléments interceptés avec les services de renseignement alliés. Dans son rapport 2016, il a indiqué que « le GCHQ a[vait] fourni des détails exhaustifs sur les modalités d'échange permettant aux partenaires du réseau Five Eyes d'accéder depuis leurs propres systèmes aux résultats de ses mandats ». Il a ajouté que ses inspecteurs avaient rencontré des représentants du réseau Five Eyes et assisté à une démonstration de la manière dont les autres membres de ce réseau pouvaient demander l'accès aux éléments interceptés en possession du GCHQ. Il a relevé, d'une part, que « [l]'accès à ces éléments interceptés [était] strictement contrôlé et [devait] être justifié dans les conditions prévues par la législation du pays hôte et les consignes de traitement énoncées dans les garanties prévues aux articles 15 et 16 » et, d'autre part, que pour pouvoir accéder aux éléments interceptés en possession du GCHQ, les analystes du réseau Five Eyes devaient suivre la même formation juridique que les agents du GCHQ (paragraphe 180 ci-dessus).

412. Au vu de ce qui précède, la Cour estime que le Commissaire à l'interception des communications exerçait une supervision indépendante et effective sur le fonctionnement du régime institué par l'article 8 § 4 de la RIPA. Le Commissaire et ses inspecteurs pouvaient notamment évaluer la nécessité et la proportionnalité d'un grand nombre de demandes de mandat et du choix ultérieur des sélecteurs, et examiner les procédures mises en place pour la conservation, le stockage ainsi que la destruction des communications interceptées et des données de communication associées. Ils pouvaient également adresser des recommandations officielles aux chefs des autorités publiques concernées, lesquelles étaient tenues de rendre compte dans un délai de deux mois des progrès accomplis dans la mise en œuvre de ces recommandations. En outre, dans ses observations devant la Grande Chambre, le Gouvernement a indiqué que le GCHQ tenait le Commissaire à l'interception régulièrement informé de la base sur laquelle il sélectionnait pour interception des canaux de transmission (paragraphes 136 et 290 ci-dessus). Les services de renseignement étaient tenus d'enregistrer chacune des étapes du processus d'interception en masse

et de laisser les inspecteurs accéder aux enregistrements en question (voir les paragraphes 6.27 et 6.28 du code de conduite en matière d'interception de communications, reproduits au paragraphe 96 ci-dessus). Enfin, le Commissaire avait aussi pour mission de superviser les échanges d'éléments interceptés avec les services de renseignement alliés (paragraphe 180 ci-dessus).

– *8. Le contrôle* a posteriori

413. Le contrôle *a posteriori* était assuré par l'IPT, qui a toujours été présidé, pendant la période sous examen, par un juge de la High Court. La chambre a conclu – et les requérantes n'ont pas contesté – que l'IPT offrait un recours effectif propre à remédier aux griefs des requérants portant soit sur des cas spécifiques de surveillance soit sur la conformité générale à la Convention d'un régime de surveillance (voir le paragraphe 265 de l'arrêt de la chambre). À cet égard, la chambre a accordé du poids au fait que l'IPT disposait d'une compétence étendue pour connaître des allégations d'interception illicite nonobstant l'absence de notification de l'interception alléguée à la personne concernée (paragraphe 122 ci-dessus). De ce fait, toute personne qui pensait avoir fait l'objet d'une surveillance secrète pouvait saisir l'IPT. Les membres de l'IPT devaient exercer ou avoir exercé de hautes fonctions judiciaires et être des juristes diplômés ayant au moins dix ans d'expérience (paragraphe 123 ci-dessus). Les personnes ayant pris part à l'autorisation ou à l'exécution d'un mandat d'interception étaient tenues de divulguer à l'IPT tous les documents qu'il jugeait utile de leur demander, y compris les documents « non publics », c'est-à-dire ceux qui, pour des raisons de sécurité nationale, ne pouvaient pas être rendus publics (paragraphe 125 ci-dessus). En outre, l'IPT pouvait tenir des audiences publiques, dans la mesure du possible (paragraphe 129 ci-dessus), et lors des audiences à huis clos, il pouvait inviter le Conseil près le Tribunal à lui soumettre des observations au nom des plaignants qui ne pouvaient pas être représentés (paragraphe 132 ci-dessus). Lorsqu'il statuait en faveur d'un plaignant, l'IPT pouvait octroyer une indemnité et ordonner toute mesure qu'il jugeait appropriée, notamment l'annulation rétroactive ou non d'un mandat et la destruction de tous les éléments obtenus dans le cadre de celui-ci (paragraphe 126 ci-dessus). Enfin, la publication des décisions de l'IPT sur son propre site internet dédié accroissait le degré de contrôle exercé sur les activités de surveillance secrète au Royaume-Uni (voir *Kennedy*, précité, § 167).

414. En outre, l'IPT était compétent pour connaître des griefs portant sur la conformité à la Convention des transferts d'éléments interceptés à des tiers ou du régime gouvernant les transferts d'éléments interceptés. En l'espèce, toutefois, les requérantes de la troisième affaire n'ont pas formulé de grief spécifique sur ce point dans le cadre de la procédure interne. Leurs griefs à l'égard de l'échange de renseignements portaient uniquement sur le

régime applicable à la réception de renseignements provenant de pays tiers (paragraphes 467-516 ci-dessous).

415. Dans ces conditions, la Cour estime que l'IPT offrait un recours juridictionnel solide à toutes les personnes qui pensaient que leurs communications avaient été interceptées par les services de renseignement.

3) Les données de communication associées

416. La Cour a déjà indiqué qu'en ce qui concerne l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications (paragraphes 363-364 ci-dessus). Au Royaume-Uni, les mandats émis en vertu de l'article 8 § 4 de la RIPA autorisaient l'interception à la fois du contenu des communications et des données de communication associées. Dans le régime découlant de l'article 8 § 4, ces dernières étaient pour l'essentiel traitées de la même manière que le contenu des communications. Il s'ensuit que le régime applicable aux données de communication souffrait des mêmes carences que celles déjà constatées au sujet du régime qui gouvernait l'interception des données de contenu (paragraphes 377, 381 et 382 ci-dessus), à savoir l'absence d'autorisation indépendante (paragraphe 377 ci-dessus), l'absence de mention des catégories de sélecteurs dans les demandes de mandat (paragraphes 381 et 382 ci-dessus), le fait que les sélecteurs liés à un individu identifiable n'étaient pas soumis à une autorisation interne préalable et le manque de prévisibilité des conditions dans lesquelles les communications pouvaient être examinées (paragraphe 391 ci-dessus) en raison à la fois de l'absence de mention des catégories de sélecteurs dans les demandes de mandat (paragraphes 381 et 382 ci-dessus) et du caractère général des certificats ministériels (paragraphe 386 ci-dessus).

417. Cependant, le traitement des données de communication bénéficiait pour l'essentiel des mêmes garanties que celles applicables aux données de contenu. Comme ces dernières, les données de communication étaient soumises à un processus de filtrage automatisé quasi instantané, à l'issue duquel une grande partie d'entre elles étaient aussitôt effacées, puis à des requêtes simples ou complexes visant à isoler celles qui étaient susceptibles de présenter un intérêt pour le renseignement. En outre, les sélecteurs utilisés pour le traitement des données de communication associées étaient encadrés par les mêmes garanties que celles applicables aux données de contenu. En particulier, les analystes avaient l'obligation de consigner les raisons pour lesquelles l'ajout d'un nouveau sélecteur au système était nécessaire et proportionné, ces mentions écrites étaient vérifiées par le

Commissaire à l'interception des communications, les sélecteurs devaient être retirés au cas où il aurait été établi qu'ils n'avaient pas été utilisés par la cible visée, et la durée pendant laquelle ils pouvaient continuer d'être utilisés avant qu'un contrôle ne soit nécessaire était limitée (paragraphe 298 ci-dessus).

418. Les données de contenu et les données de communication associées faisaient dans une large mesure l'objet des mêmes procédures en matière de conservation, d'accès, d'examen et d'utilisation, des mêmes précautions pour ce qui était de leur communication à des tiers et des mêmes procédures concernant leur effacement et leur destruction. À cet égard, les données de contenu et les données de communication associées étaient encadrées par les garanties posées par l'article 15 de la RIPA, lesquelles imposaient aux analystes qui souhaitaient accéder à des données de communication associées de rédiger une notice susceptible de contrôle expliquant pourquoi l'accès était nécessaire et proportionné au but du visé et interdisaient l'établissement de rapports de renseignement sur la base de données de communication associées tant que celles-ci n'avaient pas été examinées.

419. Toutefois, il existait deux grandes différences dans la manière dont le régime d'interception en masse traitait les données de contenu et les données de communication associées. D'abord, les données de communication associées étaient exclues de la garantie prévue à l'article 16 § 2 de la RIPA, ce qui évitait aux analystes qui souhaitaient utiliser un sélecteur lié à un individu dont on savait qu'il se trouvait dans les îles Britanniques de faire certifier par le ministre compétent que l'usage de ce sélecteur était nécessaire et proportionné au but visé. Ensuite, les données de communication associées qui ne correspondaient ni à un sélecteur fort ni à une requête complexe n'étaient pas immédiatement détruites mais étaient au contraire conservées pendant une période qui pouvait durer plusieurs mois (paragraphes 296-298 ci-dessus). La Cour doit donc rechercher si le droit interne définissait clairement les procédures à suivre en matière de sélection pour examen des données de communication associées ainsi que les limites à la durée de conservation de ces données.

420. Dans le régime institué par l'article 8 § 4, l'article 16 § 2 était la principale garantie légale encadrant le processus de sélection pour examen d'éléments interceptés, mais elle n'était pas la seule. Comme indiqué au paragraphe 417 ci-dessus, l'ajout de tout nouveau sélecteur au système devait être justifié par les analystes dans une notice expliquant pourquoi le choix du sélecteur en question était nécessaire et proportionné au but visé (paragraphes 291-292 et 298 ci-dessus), et les analystes qui souhaitaient examiner des données de communication associées devaient en plus consigner les raisons pour lesquelles cet accès était nécessaire et proportionné au but visé en vue de l'accomplissement des fonctions assignées au GCHQ par la loi (voir le paragraphe 6.4 du code de conduite en matière d'interception de communications, reproduit au paragraphe 96

ci-dessus). Ces notices étaient soumises à l'inspection et au contrôle du Commissaire à l'interception des communications (paragraphes 135-136 et 381 ci-dessus). Le Gouvernement a indiqué qu'il aurait été irréaliste d'étendre la garantie prévue à l'article 16 § 2 de la RIPA aux données de communication associées, car cela aurait contraint le ministre compétent à certifier dans chaque cas la nécessité et la proportionnalité du ciblage d'un individu. Il a ajouté que le nombre de requêtes portant sur des données de communication était bien supérieur à celui des requêtes portant sur des données de contenu (peut-être des milliers par semaine concernant des individus dont on savait ou dont on pensait qu'ils se trouvaient au Royaume-Uni) et que l'identité des individus concernés était dans bien des cas inconnue. En outre, il a précisé que les données de communication n'avaient bien souvent qu'une valeur temporaire, et que s'il avait fallu attendre l'obtention d'un mandat spécifique pour y effectuer des recherches, leur utilité du point de vue du renseignement aurait pu s'en trouver sérieusement amoindrie (paragraphe 296 ci-dessus).

421. La Cour admet que les données de communication associées constituent pour les services de renseignement un outil essentiel aux fins de la lutte contre le terrorisme et les infractions graves, et qu'en certaines circonstances, la recherche de données de communication associées liées à des personnes dont on savait qu'elles se trouvaient au Royaume-Uni et l'accès aux données en question étaient des mesures nécessaires et proportionnées. En outre, si l'article 16 § 2 de la RIPA constituait une importante garantie encadrant le processus de sélection pour examen d'éléments interceptés, il convient de relever que dans son appréciation du régime d'interception en masse de données de contenu, la Cour a accordé beaucoup plus de poids à la question de savoir s'il existait ou non un mécanisme effectif propre à garantir que le choix des sélecteurs répondait aux exigences de nécessité et de proportionnalité posées par la Convention et si ce choix faisait l'objet d'une supervision interne et externe. En conséquence, tout en rappelant les préoccupations qu'elle a exprimées aux paragraphes 381 et 382 ci-dessus au sujet du choix et de la supervision des sélecteurs, la Cour considère que l'exclusion des données de communication associées de la garantie prévue à l'article 16 § 2 de la RIPA ne revêt pas un poids décisif dans son appréciation globale.

422. En ce qui concerne la durée de conservation, le Gouvernement a avancé que les données de communication associées « exige[aient] un travail d'analyse plus important, sur une longue période, destiné à détecter des « inconnues inconnues ». Il a précisé que ce travail de détection pouvait impliquer l'agrégation de fragments de données de communication disparates en vue de la reconstitution d'un « puzzle » révélant une menace, opération qui, selon lui, nécessitait parfois l'examen d'éléments à première vue dénués d'intérêt pour le renseignement. Selon lui, ces tâches auraient été irréalisables si les données de communication non sélectionnées avaient

dû être écartées immédiatement, ou au bout de quelques jours seulement (paragraphe 297 ci-dessus).

423. Au vu de ce qui précède, et compte tenu de l'existence d'une durée maximale de conservation n'excédant pas « quelques mois » ainsi que du caractère objectivement et raisonnablement justifié de la différence de traitement, la Cour admet que les dispositions relatives à la conservation des données de communication associées étaient suffisamment sûres, même si elles différaient en substance des dispositions applicables aux données de contenu. Toutefois, les durées de conservation ici en cause n'ont été mentionnées que dans le cadre de la procédure suivie devant la Cour, si bien que l'existence de durées de conservation plus courtes n'apparaissait pas de manière évidente aux lecteurs du code de conduite en matière d'interception de communications, et il n'y était indiqué nulle part que les durées de conservation des données de communication associées différaient de celles applicables aux données de contenu. De l'avis de la Cour, pour satisfaire à l'exigence de « prévisibilité » posée par l'article 8 de la Convention, les durées de conservation mentionnées dans le cadre de la procédure suivie devant elle devraient figurer dans des dispositions législatives et/ou d'autres mesures d'ordre général.

4) Conclusion

424. La Cour admet que l'interception en masse revêt pour les États contractants une importance vitale pour détecter les menaces contre leur sécurité nationale. La Commission de Venise l'a reconnu (paragraphe 196 ci-dessus) et le gouvernement défendeur a défendu cette position, de même que les gouvernements français et néerlandais dans leurs tierces interventions (paragraphes 300 et 303 ci-dessus). Le Contrôleur indépendant de la législation sur le terrorisme est parvenu à la même conclusion. Après avoir examiné de nombreux éléments confidentiels, il a estimé que l'interception en masse constituait un moyen d'action essentiel, d'une part parce que les terroristes, les criminels et les services de renseignement étrangers hostiles disposaient de capacités de plus en plus sophistiquées pour échapper à la détection opérée par des moyens classiques et, d'autre part, parce que la nature mondiale d'Internet avait pour conséquence que la voie empruntée par une communication donnée était devenue fortement imprévisible. Après examen d'autres techniques que l'interception en masse (notamment les interceptions ciblées, le recours au renseignement humain et l'utilisation d'outils de cyberdéfense commerciaux), le Contrôleur et son équipe ont conclu qu'aucune d'entre elles, prises isolément ou combinées, n'aurait été suffisante pour remplacer l'interception en masse (paragraphe 166 ci-dessus).

425. Cela étant, la Cour rappelle que l'interception en masse recèle un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée (paragraphe 347 ci-dessus). Elle

estime en conséquence que dans un État régi par la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8 (*Roman Zakharov*, précité, § 228), le régime découlant de l'article 8 § 4 de la RIPA, considéré dans son ensemble, ne renfermait pas suffisamment de garanties « de bout en bout » pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus, en dépit des garde-fous qu'il comportait, dont certains ont été jugés solides (voir, par exemple, les paragraphes 412 et 415 ci-dessus). Elle relève notamment que ce régime présentait des lacunes fondamentales, à savoir l'absence d'autorisation indépendante, l'absence de mention des catégories de sélecteurs dans les demandes de mandat et le fait que les sélecteurs liés à un individu n'étaient pas soumis à une autorisation interne préalable (paragraphes 377-382 ci-dessus). Ces insuffisances affectaient non seulement l'interception du contenu des communications, mais aussi l'interception des données de communication associées (paragraphe 416 ci-dessus). Si la supervision indépendante et effective exercée sur le régime par le Commissaire à l'interception des communications et le recours juridictionnel solide que l'IPT offrait à toutes les personnes pensant que leurs communications avaient été interceptées par les services de renseignement constituaient des garanties importantes, celles-ci n'étaient pas suffisantes pour contrebalancer les lacunes mises en évidence aux paragraphes 377-382 ci-dessus.

426. Eu égard aux lacunes constatées ci-dessus, la Cour conclut que l'article 8 § 4 de la RIPA ne répondait pas à l'exigence de « qualité de la loi » et ne permettait donc pas de circonscrire l'« ingérence » au niveau « nécessaire dans une société démocratique ».

427. Partant, il y a eu violation de l'article 8 de la Convention à cet égard.

C. Sur la violation alléguée de l'article 10 de la Convention

428. Invoquant l'article 10 de la Convention, les requérantes de la deuxième et de la troisième affaire se plaignaient du régime découlant de l'article 8 § 4 de la RIPA. Faisant valoir leurs qualités respectives de journalistes et d'ONG, elles avançaient que la protection garantie par l'article 10 aux communications couvertes par le secret professionnel revêtait pour elles une importance cruciale. Toutefois, la chambre ayant déclaré irrecevable pour non-épuisement des voies de recours internes le grief formulé par les requérantes de la troisième affaire, l'objet de l'affaire renvoyée devant la Grande Chambre se limite au grief de violation de l'article 10 dans le chef des journalistes.

429. L'article 10 de la Convention est ainsi libellé :

> « 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées

sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »

1. L'arrêt de la chambre

430. La chambre a conclu que dès lors que les mesures de surveillance relevant du régime institué par l'article 8 § 4 de la RIPA ne visaient pas à surveiller les journalistes ni à découvrir leurs sources, l'interception de ces communications ne pouvait, en elle-même, être qualifiée d'atteinte particulièrement grave à la liberté d'expression. Elle a cependant ajouté que l'atteinte aurait été plus forte si ces communications avaient été sélectionnées pour examen et qu'elle n'aurait pu alors se justifier par « un impératif prépondérant d'intérêt public » que si elle était accompagnée de garanties suffisantes. À cet égard, elle a notamment indiqué que les circonstances dans lesquelles on pouvait sélectionner les communications pour examen intentionnellement devaient être précisées avec une clarté suffisante dans le droit interne et que des mesures adéquates devaient être mises en place pour garantir la protection de la confidentialité après cette sélection, qu'elle fût intentionnelle ou non. En l'absence de toute modalité divulguée au public qui aurait limité la capacité des services de renseignement à lancer des recherches dans les éléments journalistiques confidentiels et à les examiner à moins que cela ne fût « justifié par un impératif prépondérant d'intérêt public », la chambre a conclu qu'il y avait aussi eu violation de l'article 10 de la Convention.

2. Thèses des parties et observations des tiers intervenants

a) Les requérantes

431. Les requérantes de la deuxième affaire soutiennent que le régime d'interception en masse était contraire à l'article 10 parce que l'interception à grande échelle et la conservation de grandes bases de données avaient un effet dissuasif sur la liberté de communication des journalistes.

432. Compte tenu de l'importance fondamentale que revêt la liberté de la presse, les requérantes considèrent que toute ingérence dans la liberté journalistique, s'agissant en particulier du droit de préserver la confidentialité des sources, doit être entourée de garanties procédurales prévues par la loi correspondant à l'importance du principe en jeu. En particulier, selon elles, l'expression « prévue par la loi » veut que toute

mesure permettant d'identifier des sources journalistiques ou de révéler des éléments journalistiques soit autorisée par un juge ou un autre organe décisionnel indépendant et impartial. Ce contrôle devrait être exercé *a priori* et l'organe décisionnel devrait être habilité à déterminer si la mesure est justifiée « par un impératif prépondérant d'intérêt public » et, en particulier, si une mesure moins intrusive aurait suffi à satisfaire un tel impératif (*Sanoma Uitgevers B.V. c. Pays-Bas* [GC], n° 38224/03, 14 septembre 2010). Or le régime institué par l'article 8 § 4 de la RIPA n'aurait offert aucune de ces garanties.

b) Le Gouvernement

433. Le Gouvernement soutient tout d'abord que rien dans la jurisprudence de la Cour ne permet de dire que la mise en œuvre d'un régime de surveillance stratégique doit être soumise à une autorisation judiciaire (ou indépendante) préalable au motif que certains éléments journalistiques pourraient être interceptés dans ce cadre. Il affirme que la Cour a au contraire établi une nette distinction entre la surveillance stratégique des communications et/ou des données de communication, au cours de laquelle il est possible que certains éléments journalistiques se trouvent accidentellement « pris dans les filets » des interceptions, d'une part, et les mesures ciblant des éléments journalistiques, d'autre part (voir *Weber et Saravia*, décision précitée, § 151 ; et, *a contrario*, *Sanoma Uitgevers B.V.*, précité, et *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, n° 39315/06, 22 novembre 2012). En effet, l'exigence d'une autorisation judiciaire préalable n'aurait aucun sens dans le domaine de l'interception en masse puisque la possibilité que l'exécution d'un mandat conduise à l'interception de certains éléments journalistiques confidentiels serait la seule indication pouvant être donnée au juge.

434. Cela étant, le Gouvernement souscrit à la conclusion de la chambre selon laquelle un renforcement de la protection s'impose au stade de la sélection pour examen. Il confirme que le code de conduite en matière d'interception de communications a été modifié et que le passage pertinent de ce texte est ainsi libellé : « [u]ne attention particulière doit être accordée à l'interception de communications ou à la sélection pour examen de contenus renfermant des informations dont on peut raisonnablement penser qu'elles présentent un haut degré de confidentialité. Il s'agit notamment des communications renfermant des informations couvertes par le secret professionnel des avocats, des éléments journalistiques confidentiels ou des communications permettant d'identifier une source journalistique ».

c) Les tiers intervenants

i. Le gouvernement français

435. Le gouvernement français avance que l'article 10 de la Convention ne s'oppose pas à la surveillance de journalistes à condition que pareille mesure poursuive un but légitime, qu'elle soit nécessaire, qu'elle ne vise pas les journalistes et qu'elle ne soit pas destinée à découvrir des sources journalistiques. Selon lui, aucun parallèle ne peut être établi entre l'hypothèse où les communications d'un journaliste sont accidentellement interceptées et la situation dans laquelle une décision des autorités nationales impose à un journaliste de divulguer ses sources.

ii. Le gouvernement du Royaume de Norvège

436. Le gouvernement norvégien soutient que dès lors que les États bénéficient, au regard de l'article 8, d'une ample marge d'appréciation pour décider de la mise en place d'un régime d'interception en masse, il doit en toute logique en aller de même sur le terrain de l'article 10. Il avance que si la Cour devait subordonner la mise en place d'un régime d'interception en masse à l'existence d'une justification fondée sur « un impératif prépondérant d'intérêt public » au seul motif que certaines des communications interceptées peuvent avoir trait à des échanges avec des journalistes, la nature et les buts d'un tel régime s'en trouveraient compromis.

iii. Le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression

437. Le rapporteur spécial avance que les mesures de surveillance portent atteinte au droit à la liberté d'expression et qu'elles doivent en conséquence satisfaire à l'article 19 § 3 du PIDCP, lequel exige que les restrictions éventuelles à ce droit soient « expressément fixées par la loi et (...) nécessaires » au respect des droits ou de la réputation d'autrui, ou à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques. Il signale que les programmes de surveillance de masse posent de redoutables défis du point de vue de l'exigence d'accessibilité de la loi en raison de la complexité du fonctionnement des technologies de surveillance, de l'imprécision des normes juridiques régissant l'interception des communications et du caractère complexe – et souvent secret – des structures administratives concernées. En outre, il indique que ces programmes posent un sérieux problème de proportionnalité du point de vue de l'ingérence dans le travail des journalistes et de la protection de leurs sources. Dès lors, selon lui, que le droit des droits de l'homme garantit à la confidentialité un niveau de protection élevé, les restrictions dans ce domaine devraient être exceptionnelles et appliquées uniquement par des autorités judiciaires, et le recours à des moyens de contournement en vue de

lever la confidentialité d'une source devrait être proscrit, à moins d'avoir été autorisé par l'autorité judiciaire sur la base de règles claires et étroitement délimitées. À cet égard, la portée de la protection accordée aux communications confidentielles devrait tenir compte de l'interprétation large que le PIDCP donne au terme « journaliste ».

iv. Article 19

438. Article 19 exhorte la Cour à accorder aux ONG la même protection que celle qu'elle accorde ordinairement aux journalistes.

v. La Fondation Helsinki pour les droits de l'homme (« la Fondation Helsinki »)

439. La Fondation Helsinki estime que la protection des sources journalistiques est affaiblie non seulement par la surveillance du contenu des communications des journalistes, mais aussi par la surveillance des métadonnées correspondantes, lesquelles pourraient à elles seules permettre l'identification de sources et d'informateurs. Il serait particulièrement problématique que des informations confidentielles puissent être acquises en dehors de tout contrôle des journalistes et à leur insu, ce qui les priverait de leur droit d'invoquer la confidentialité et empêcherait leurs sources de se fier aux garanties de confidentialité qu'ils leur donneraient.

vi. La Media Lawyers' Association (« la MLA »)

440. La MLA se dit préoccupée par la capacité des régimes de surveillance de masse à intercepter des communications de journalistes et des données de communication permettant l'identification des sources journalistiques. Elle estime que l'interception d'éléments journalistiques est en soi susceptible d'enfreindre l'article 10 de la Convention, même si ceux-ci ne sont pas analysés. En conséquence, elle considère que des garanties appropriées doivent être impérativement mises en place pour protéger la confidentialité des sources journalistiques, quel que soit le but de la collecte d'informations. En outre, elle avance que les régimes qui permettent aux États d'intercepter les communications des journalistes sans autorisation judiciaire préalable sont plus susceptibles d'affecter le journalisme d'intérêt public car, du fait de la nature des articles publiés, l'identification des sources présente pour les États un intérêt particulier. Ce risque serait particulièrement important lorsque la source est un fonctionnaire lanceur d'alerte. La simple éventualité que ce type de source puisse être identifiée aurait un effet dissuasif non négligeable. Il faudrait donc, à tout le moins, que l'article 10 soit interprété comme exigeant que toute tentative d'obtention d'éléments journalistiques ou d'identification de sources journalistiques soit soumise à une autorisation judiciaire préalable dans le cadre d'une procédure contradictoire.

vii. Le syndicat britannique des journalistes (National Union of Journalists) et la Fédération internationale des journalistes

441. Le syndicat britannique des journalistes et la Fédération internationale des journalistes estiment que la confidentialité des sources est indispensable à la liberté de la presse. Ils se disent aussi préoccupés par la possibilité que le Royaume-Uni échange des données conservées avec d'autres pays. Ils soulignent à cet égard que si des éléments journalistiques confidentiels venaient à être partagés avec un pays dont on ne peut pas être certain qu'il en assurera la sécurité, ils pourraient finir entre les mains de personnes qui pourraient s'en prendre au journaliste ou à sa source. Ils considèrent que les garanties figurant dans la version mise à jour des codes de conduite sur l'interception de communications et l'acquisition de données de communication ne sont pas adéquates, en particulier dans les cas où la cible de la mesure de surveillance n'est pas le journaliste ou l'identification de sa source.

3. Appréciation de la Cour

a) Principes généraux relatifs à la protection des sources des journalistes

442. La liberté d'expression constituant l'un des fondements essentiels d'une société démocratique, la Cour a toujours soumis à un examen particulièrement vigilant les garanties du respect de la liberté d'expression dans les affaires relevant de l'article 10 de la Convention. Les garanties à accorder à la presse revêtent une importance particulière, et la protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse. L'absence d'une telle protection pourrait dissuader les sources journalistiques d'aider la presse à informer le public sur des questions d'intérêt général. En conséquence, la presse pourrait être moins à même de jouer son rôle indispensable de « chien de garde » et son aptitude à fournir des informations précises et fiables pourrait s'en trouver amoindrie (voir, entre autres, *Goodwin c. Royaume-Uni*, n° 17488/90, § 39, 27 mars 1996, *Sanoma Uitgevers B.V.*, précité, § 50, et *Weber et Saravia*, décision précitée, § 143).

443. Une injonction de divulgation des sources peut avoir un impact préjudiciable non seulement sur les sources, dont l'identité peut être révélée, mais également sur le journal ou toute autre publication visés par l'injonction, dont la réputation auprès des sources potentielles futures peut être affectée négativement par la divulgation, et sur les membres du public, qui ont un intérêt à recevoir les informations communiquées par des sources anonymes. Toutefois, il y a « une différence fondamentale » entre le fait pour les autorités d'ordonner à un journaliste de révéler l'identité de ses sources et le fait qu'elles mènent des perquisitions au domicile et sur le lieu de travail de celui-ci afin de découvrir ses sources (comparer *Goodwin*, précité, § 39, avec *Roemen et Schmit c. Luxembourg*, n° 51772/99, § 57,

CEDH 2003-IV). Même si elle reste sans résultat, la perquisition constitue un acte plus grave qu'une sommation de divulgation de l'identité de la source, car les enquêteurs qui investissent le lieu de travail d'un journaliste ont accès à toute la documentation détenue par celui-ci (*Roemen et Schmit*, précité, § 57).

444. Une atteinte à la protection des sources journalistiques ne peut être jugée compatible avec l'article 10 de la Convention que si elle est justifiée par un impératif prépondérant d'intérêt public (voir *Sanoma Uitgevers B.V.*, précité, § 51, *Goodwin*, précité, § 39, *Roemen et Schmit*, précité, § 46, et *Voskuil c. Pays-Bas*, nº 64752/01, § 65, 22 novembre 2007). En outre, toute atteinte au droit à la protection des sources journalistiques doit être entourée de garanties procédurales, définies par la loi, en rapport avec l'importance du principe en jeu (*Sanoma Uitgevers B.V.*, précité, §§ 88-89). Au premier rang des garanties exigées doit figurer la possibilité de faire contrôler la mesure par un juge ou tout autre organe décisionnel indépendant et impartial investi du pouvoir de dire, avant la remise des éléments réclamés, s'il existe un impératif d'intérêt public l'emportant sur le principe de protection des sources des journalistes et, dans le cas contraire, d'empêcher tout accès non indispensable aux informations susceptibles de conduire à la divulgation de l'identité des sources (*Sanoma Uitgevers B.V.*, précité, §§ 88-90).

445. Eu égard à la nécessité d'un contrôle de nature préventive, le juge ou autre organe indépendant et impartial doit donc être en mesure d'effectuer avant toute divulgation cette mise en balance des risques potentiels et des intérêts respectifs relativement aux éléments dont la divulgation est demandée, de sorte que les arguments des autorités désireuses d'obtenir la divulgation puissent être correctement appréciés. La décision à prendre doit être régie par des critères clairs, notamment quant au point de savoir si une mesure moins intrusive peut suffire pour servir les intérêts publics prépondérants ayant été établis. Le juge ou autre organe compétent doit avoir la faculté de refuser de délivrer une injonction de divulgation ou d'émettre une injonction de portée plus limitée ou plus encadrée, de manière à ce que les sources concernées puissent échapper à la divulgation de leur identité, qu'elles soient ou non spécifiquement nommées dans les éléments dont la remise est demandée, au motif que la communication de pareils éléments créerait un risque sérieux de compromettre l'identité de sources de journalistes (voir *Sanoma Uitgevers B.V.*, précité, § 92, et *Nordisk Film & TV A/S v. Danemark* (déc.), nº 40485/02, CEDH 2005-XIII). En cas d'urgence, une procédure doit pouvoir être suivie qui permette d'identifier et d'isoler, avant qu'elles ne soient exploitées par les autorités, les informations susceptibles de permettre l'identification des sources de celles qui n'emportent pas semblable risque (voir, *mutatis mutandis*, *Wieser et Bicos Beteiligungen GmbH c. Autriche*, nº 74336/01, §§ 62-66, CEDH 2007‑XI).

b) L’article 10 dans le contexte de l’interception en masse

446. Dans l’affaire *Weber et Saravia*, la Cour a estimé que le régime de « surveillance stratégique » litigieux avait porté atteinte au droit à la liberté d’expression dont la première requérante jouissait en qualité de journaliste, mais elle a jugé que le fait que les mesures de surveillance ne visaient pas à surveiller les journalistes ni à découvrir des sources journalistiques était déterminant. Elle en a conclu que l’ingérence dans la liberté d’expression de la première requérante ne pouvait être qualifiée de particulièrement grave, et que les griefs de l’intéressée devaient être rejetés pour défaut manifeste de fondement (*Weber et Saravia*, décision précitée, §§ 143 à 145 et 151).

c) L’approche à adopter en l’espèce

447. Le régime institué par l’article 8 § 4 de la RIPA permettait aux services de renseignement d’accéder à des éléments journalistiques confidentiels de manière intentionnelle, en utilisant délibérément des sélecteurs ou des termes de recherche liés à un journaliste ou à un organe de presse, ou de manière fortuite, en prenant accidentellement de tels éléments dans les « filets » d’une interception en masse.

448. Lorsque les services de renseignement cherchent à accéder à des éléments journalistiques confidentiels, par exemple en utilisant délibérément un sélecteur fort lié à un journaliste, ou qu’il est très probable, compte tenu des sélecteurs forts qui ont été choisis, que de tels éléments seront sélectionnés pour examen, la Cour estime que l’ingérence qui en découle est comparable à celle qui résulterait d’une perquisition au domicile ou sur le lieu de travail d’un journaliste. En effet, indépendamment de la question de savoir si les services de renseignement cherchent ou non à identifier une source, il est très probable que l’utilisation de sélecteurs forts ou de termes de recherche liés à un journaliste aboutira à la collecte de très nombreux éléments journalistiques confidentiels, mesure plus attentatoire encore à la protection des sources qu’une injonction de divulgation de l’identité d’une source (*Roemen et Schmit*, précité, § 57). En conséquence, la Cour estime qu’avant que les services de renseignement ne puissent utiliser des sélecteurs ou des termes de recherche dont on sait qu’ils sont liés à un journaliste ou qui aboutiront en toute probabilité à la sélection pour examen d’éléments journalistiques confidentiels, ces sélecteurs ou termes de recherche doivent avoir été autorisés par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si cette mesure est « justifiée par un impératif prépondérant d’intérêt public » et, en particulier, si une mesure moins intrusive suffirait à satisfaire un tel impératif (*Sanoma Uitgevers B.V.*, précité, §§ 90 à 92).

449. Même en l’absence d’intention d’accéder à des éléments journalistiques confidentiels, et même en l’absence de sélecteurs ou de termes de recherche rendant très probable la sélection pour examen

d'éléments journalistiques confidentiels, il existe néanmoins un risque que de tels éléments soient interceptés, voire examinés, en se trouvant accidentellement « pris dans les filets » d'une interception de masse. La Cour estime que pareille situation diffère matériellement de la mise en place d'une surveillance ciblée d'un journaliste en vertu du régime découlant de l'article 8 § 1 ou de l'article 8 § 4 de la RIPA. L'interception éventuelle de communications journalistiques étant en pareil cas involontaire, il est impossible de prévoir d'emblée l'importance de l'atteinte portée à ces communications et/ou sources journalistiques. Dans ces conditions, un juge ou un autre organe indépendant ne serait pas en mesure de déterminer, au stade de l'autorisation, si une telle atteinte est ou non « justifiée par un impératif prépondérant d'intérêt public » et, en particulier, si une mesure moins intrusive suffirait à satisfaire un tel impératif.

450. Dans l'affaire *Weber et Saravia*, la Cour a jugé que l'ingérence dans la liberté d'expression résultant de la surveillance stratégique litigieuse ne pouvait être qualifiée de particulièrement grave dès lors qu'elle ne visait pas à surveiller des journalistes et que les autorités ne pouvaient découvrir que les conversations d'un journaliste avaient été surveillées qu'au moment où elles examinaient, le cas échéant, les télécommunications interceptées (*Weber et Saravia*, décision précitée, § 151). En conséquence, elle a conclu que l'interception initiale, sans examen des éléments interceptés, ne portait pas gravement atteinte à l'article 10 de la Convention. Toutefois, comme la Cour l'a constaté plus haut, à l'époque actuelle, où le numérique est de plus en plus présent, les capacités technologiques ont considérablement accru le volume des communications transitant par Internet au niveau mondial, si bien que la surveillance qui ne vise pas directement les individus est susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère (paragraphes 322-323 ci-dessus). L'examen de communications journalistiques ou de données de communication associées par un analyste pouvant conduire à l'identification d'une source, la Cour estime que le droit interne doit impérativement comporter des garanties solides en ce qui concerne la conservation, l'examen, l'utilisation, la transmission à des tiers et la destruction de ces éléments confidentiels. En outre, lorsqu'il apparaît que des communications journalistiques ou des données de communication associées n'ayant pas été sélectionnées pour examen par l'utilisation délibérée d'un sélecteur ou d'un terme de recherche dont on sait qu'il est lié à un journaliste contiennent malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne devraient être possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures sont « justifiées par un impératif prépondérant d'intérêt public ».

d) Application des critères susmentionnés aux faits de l'espèce

451. Dans l'affaire *Weber et Saravia*, la Cour a expressément reconnu que le régime de surveillance litigieux avait porté atteinte au droit à la liberté d'expression dont la première requérante jouissait en qualité de journaliste (*Weber et Saravia*, décision précitée, §§ 143-145). Dans la présente affaire, la Cour a conclu que le fonctionnement du régime institué par l'article 8 § 4 de la RIPA s'analysait en une ingérence dans les droits de l'ensemble des requérantes tels que garantis par l'article 8 de la Convention (paragraphes 324-331 ci-dessus). Les requérantes de la deuxième affaire ayant respectivement la qualité d'association de journalistes et de journaliste, la Cour conclut que le régime institué par l'article 8 § 4 de la RIPA s'analysait aussi en une ingérence dans le droit à la liberté d'expression dont les intéressées jouissaient en qualité de journalistes en vertu de l'article 10 de la Convention.

452. Comme indiqué ci-dessus, le régime institué par l'article 8 § 4 de la RIPA avait une base claire en droit interne (paragraphes 365 et 366 ci-dessus). Toutefois, au cours de son examen de la prévisibilité et de la nécessité de régime sous l'angle de l'article 8 de la Convention, la Cour a constaté que celui-ci et les garanties qu'il comportait présentaient un certain nombre de lacunes, à savoir l'absence d'autorisation indépendante (paragraphe 377 ci-dessus), l'absence d'identification des catégories de sélecteurs dans les demandes de mandat (paragraphes 381-382 ci-dessus) et l'absence d'autorisation interne préalable des sélecteurs liés à un individu identifiable (paragraphe 382 ci-dessus).

453. Néanmoins, les éléments journalistiques confidentiels étaient protégés par plusieurs garanties supplémentaires énoncées aux paragraphes 4.1 à 4.3 et 4.26 à 4.31 du code de conduite en matière d'interception de communications (paragraphe 96 ci-dessus). En vertu du paragraphe 4.1, les demandes de mandat d'interception devaient préciser si l'interception comportait un risque d'atteinte collatérale au droit à la vie privée – notamment lorsqu'étaient en cause des communications journalistiques – et, dans la mesure du possible, les mesures à prendre en vue de réduire la portée de l'intrusion collatérale. Toutefois, ce paragraphe n'obligeait le ministre compétent à tenir compte de ces circonstances et de ces mesures que dans le cadre de l'examen des demandes de mandat relevant de l'article 8 § 1 de la RIPA, c'est-à-dire d'un mandat autorisant une interception ciblée. Par ailleurs, le paragraphe 4.2 lui imposait d'« apporter une attention particulière » aux communications pouvant porter sur des éléments journalistiques confidentiels, et le paragraphe 4.26 indiquait que l'interception de communications portant sur des éléments journalistiques confidentiels appelait une « attention particulière ».

454. Le Gouvernement indique que les éléments journalistiques confidentiels relevaient également du champ d'application du paragraphe 4.28 du code de conduite en matière d'interception de

communications, lequel énonçait que lorsque la mesure envisagée visait à permettre l'acquisition d'informations *personnelles* confidentielles, les motifs sur lesquels elle reposait, sa nécessité et sa proportionnalité devaient être clairement précisés. Cette disposition prévoyait également que si l'acquisition de telles informations était probable mais non recherchée, toutes les possibilités d'atténuation de ce risque devaient être envisagées, et que s'il n'en existait aucune, il fallait réfléchir à la nécessité de mettre en place des procédures spéciales pour le traitement de ces informations au sein de l'agence interceptrice (paragraphe 96 ci-dessus). Toutefois, la Cour relève que dans le paragraphe 4.26 du même code, les « informations personnelles confidentielles » semblent se différencier des « éléments journalistiques confidentiels » (paragraphe 96 ci-dessus).

455. En ce qui concerne la conservation d'éléments confidentiels, le paragraphe 4.29 du code de conduite en matière d'interception de communications prévoyait que ces éléments ne pouvaient être conservés que lorsque cette mesure était nécessaire et proportionnée à l'un des buts autorisés visés à l'article 15 § 4 de la RIPA, et qu'ils devaient être détruits de manière sécurisée lorsqu'ils n'étaient plus nécessaires dans l'un de ces buts (paragraphe 96 ci-dessus). De plus, le paragraphe 4.30 énonçait que si ces éléments étaient conservés ou transmis à un organe externe, il fallait prendre des mesures raisonnables pour signaler leur caractère confidentiel, et qu'en cas de doute quant à la licéité de la transmission envisagée d'informations confidentielles, un conseiller juridique de l'agence interceptrice concernée devait être consulté avant la poursuite de la transmission (paragraphe 96 ci-dessus). Enfin, le paragraphe 4.31 imposait de signaler au Commissaire à l'interception des communications que de tels éléments avaient été conservés dès qu'il était raisonnablement possible de le faire, et de mettre ces éléments à sa disposition à sa demande (paragraphe 96 ci-dessus).

456. Au vu de ce qui précède, la Cour admet que les garanties relatives à la conservation, à la transmission à des tiers et à la destruction des éléments journalistiques confidentiels prévues par le code de conduite en matière d'interception de communications étaient adéquates. Toutefois, les garanties supplémentaires énoncées dans ce code ne remédiaient pas aux lacunes mises en évidence par la Cour dans son analyse du régime litigieux sous l'angle de l'article 8 de la Convention, et elles ne satisfaisaient pas non plus aux exigences posées par elle aux paragraphes 448-450 ci-dessus. En particulier, elles ne prévoyaient nullement que l'utilisation de sélecteurs ou de termes de recherche dont on savait qu'ils étaient liés à un journaliste devait être autorisée par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si cette mesure était « justifiée par un impératif prépondérant d'intérêt public » et si une mesure moins intrusive aurait suffi à satisfaire un tel impératif. Au contraire, lorsque la mesure envisagée visait à permettre l'accès à des éléments journalistiques

confidentiels, ou que l'accès à de tels éléments était hautement probable compte tenu de l'utilisation de sélecteurs liés à un journaliste, il était seulement exigé que les motifs sur lesquels elle reposait, sa nécessité et sa proportionnalité soient clairement précisés.

457. En outre, le régime litigieux ne comportait pas de garde-fous suffisants garantissant que, lorsqu'il apparaissait que des communications n'ayant pas été sélectionnées pour examen par l'utilisation délibérée d'un sélecteur ou d'un terme de recherche dont on savait qu'il était lié à un journaliste contenaient malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne seraient possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures étaient « justifiées par un impératif prépondérant d'intérêt public ». Au lieu de cela, le paragraphe 4.2 du code de conduite en matière d'interception de communications se bornait à exiger qu'une « attention particulière » soit apportée à l'interception de communications qui risquaient de contenir des éléments journalistiques confidentiels, et que toutes les possibilités d'atténuation de ce risque soient envisagées (paragraphe 96 ci-dessus).

458. Eu égard à ces lacunes et à celles mises en évidence par la Cour dans son analyse du grief de violation de l'article 8 de la Convention, force est de conclure que le fonctionnement du régime institué par l'article 8 § 4 de la RIPA emportait également violation de l'article 10 de la Convention.

III. SUR LA RÉCEPTION DE RENSEIGNEMENTS PROVENANT DE SERVICES DE RENSEIGNEMENT ÉTRANGERS

A. Sur l'article 8 de la Convention

459. Les requérantes de la première affaire se plaignent de la réception, par le Royaume-Uni, d'éléments provenant de services de renseignement étrangers. Les requérantes de la troisième affaire soutiennent plus particulièrement que la réception, par l'État défendeur, d'éléments interceptés par la NSA dans le cadre des programmes PRISM ou Upstream était contraire à leurs droits découlant de l'article 8 de la Convention.

1. Sur l'objet du grief porté devant la Grande Chambre

460. Dans l'affaire *Liberty*, l'IPT a classé les éléments que le Royaume-Uni était susceptible de recevoir de services de renseignement étrangers alliés en trois catégories, à savoir les éléments dont l'interception n'avait pas été sollicitée, les éléments dont l'interception avait été sollicitée et les éléments ne provenant pas d'une interception. La chambre ayant été informé par le Gouvernement qu'il était « peu probable et rare » que des éléments interceptés soient communiqués aux autorités britanniques sans que celles-ci

n'en aient fait la demande, elle n'a pas examiné les éléments relevant de cette catégorie (voir le paragraphe 417 de l'arrêt de la chambre). Elle a également refusé d'examiner la question de la réception d'éléments ne provenant pas d'une interception, au motif que les requérantes n'avaient pas indiqué quel type d'éléments les services de renseignement étrangers auraient pu obtenir par des méthodes autres que l'interception et qu'elles n'avaient donc pas démontré qu'une telle acquisition aurait pu porter atteinte à leurs droits garantis par l'article 8 (voir le paragraphe 449 de l'arrêt de la chambre). Les requérantes n'ont pas contesté les conclusions auxquelles la chambre est parvenue sur ces deux points.

461. En outre, l'affaire *Liberty* ayant été introduite par les requérantes de la troisième affaire, l'IPT s'est borné à examiner la question de la réception de renseignements provenant de la NSA. Dans leurs observations devant la chambre et la Grande Chambre, les parties ont également axé leur argumentation sur la réception de renseignements provenant de la NSA.

462. En conséquence, la Grande Chambre se bornera à examiner le grief tiré de la réception d'éléments dont l'interception avait été sollicitée auprès de la NSA.

2. Sur l'exception préliminaire du Gouvernement

463. Le Gouvernement soutient que les requérantes de la première et de la troisième affaire ne peuvent se prétendre victimes de la violation alléguée, au motif selon lui qu'aucune des deux conditions posées dans l'arrêt *Roman Zakharov* (précité, § 171) n'est satisfaite dès lors que les intéressées n'avaient pu en aucune manière être affectées par la législation permettant la mise en place de mesures de surveillance secrète et qu'elles disposaient de recours en droit interne. Il soutient en particulier que les requérantes n'ont avancé aucun argument donnant à penser qu'elles avaient été exposées à un risque réel de voir leurs communications interceptées dans le cadre des programmes PRISM ou Upstream ou sollicitées par les services de renseignement britanniques. En outre, les requérantes auraient disposé au niveau national d'une voie de droit effective pour découvrir si elles avaient fait l'objet d'un échange de renseignements illicite.

a) L'arrêt de la chambre

464. Après avoir admis que le recours ouvert devant l'IPT aurait été un recours effectif pour le grief de violation de la Convention formulé par les requérantes, la chambre a jugé que celles-ci ne pouvaient se prétendre « victimes » d'une violation découlant de la simple existence du régime d'échange de renseignements que si elles étaient en mesure de démontrer qu'elles étaient potentiellement exposées au risque que les autorités britanniques obtiennent leurs données de communication en les demandant à un service de renseignement étranger (voir les paragraphes 392-393 de

l'arrêt de la chambre, qui renvoient à l'arrêt *Roman Zakharov*, précité, § 171).

465. Sur la base des informations qui lui avaient été communiquées, la chambre a jugé qu'il y avait potentiellement un risque que les communications des requérantes aient été obtenues par un service de renseignement étranger et demandées par les autorités britanniques à un service de renseignement étranger (voir le paragraphe 395 de l'arrêt de la chambre). Elle a relevé que si la possibilité, pour les autorités britanniques, de demander à un service de renseignement étranger les communications des requérantes était subordonnée à l'existence d'un mandat émis en vertu de l'article 8 § 1 ou de l'article 8 § 4, il ressortait clairement de l'affaire *Liberty* que les communications d'au moins deux des requérantes de la troisième affaire avaient été légalement interceptées et sélectionnées pour examen par les services de renseignement du Royaume-Uni en application du régime découlant de l'article 8 § 4 de la RIPA. Elle a observé que même s'il n'y avait pas de raison de croire que ces requérantes aient elles-mêmes présenté un intérêt pour les services de renseignement, leurs communications pouvaient avoir été obtenues légalement en vertu du régime découlant de l'article 8 § 4 de la RIPA si, comme elles l'affirmaient, elles avaient été en contact avec des personnes présentant un tel intérêt. De même, les communications de ces requérantes pouvaient avoir été légalement demandées à un pays étranger en vertu du régime d'échange de renseignements si les intéressées avaient été en contact avec un individu faisant l'objet d'une telle demande.

466. Ayant observé que le fonctionnement d'Upstream était similaire à celui du régime institué par l'article 8 § 4 de la RIPA, la chambre a admis qu'il y avait potentiellement un risque que les communications des requérantes aient été obtenues par la NSA.

b) Appréciation de la Cour

467. Les requérantes de contestent pas la conclusion de la chambre selon laquelle l'IPT offrait un recours interne effectif pour les griefs de violation de la Convention dirigés contre le fonctionnement d'un régime de surveillance. Pour les raisons exposées aux paragraphes 413-415 ci-dessus, la Grande Chambre souscrit à cette conclusion. En conséquence, comme l'a relevé la chambre, les requérantes ne peuvent se prétendre « victimes » d'une violation découlant de la simple existence du régime d'échange de renseignements que si elles sont en mesure de démontrer qu'elles étaient potentiellement exposées au risque que les autorités britanniques obtiennent leurs communications en les demandant à un service de renseignement étranger (*Roman Zakharov*, précité, § 171). Tel ne sera le cas que si les requérantes étaient potentiellement exposées au risque, d'une part, que leurs communications aient été interceptées par un service de renseignement étranger et, d'autre part, que celles-ci aient été demandées par le GCHQ.

468. S'attachant à la question de la réception de renseignements provenant des États-Unis, le Gouvernement soutient que les requérantes n'étaient pas potentiellement exposées au risque d'une interception de leurs communications par Upstream, car celui-ci est un régime d'interceptions ciblées. Toutefois, la NSA a expliqué qu'avant avril 2017, Upstream collectait des communications à destination ou en provenance de sélecteurs relevant de l'article 702 (tels que des adresses électroniques) ou en rapport avec de tels sélecteurs, et que ce n'était que depuis cette époque qu'il se limitait à intercepter des communications à destination ou en provenance de tels sélecteurs (paragraphe 263 ci-dessus). Les sélecteurs relevant de l'article 702 étant appliqués à toutes les communications transitant par certains câbles précis, Upstream n'est guère différent du régime institué par l'article 8 § 4 de la RIPA, qui permettait l'interception de toutes les communications transitant par certains câbles et leur filtrage au moyen de sélecteurs. La seule différence apparente entre les deux régimes réside dans le fait que depuis 2017, la NSA ne peut effectuer que des recherches sur des communications à destination ou en provenance d'un sélecteur fort, tandis que le GCHQ demeure habilité à effectuer des recherches au moyen de requêtes complexes.

469. Dans l'affaire *Liberty*, l'IPT a confirmé qu'un certain nombre de communications d'au moins deux des requérantes de la troisième affaire avaient non seulement été interceptées en vertu d'un mandat émis en vertu de l'article 8 § 4 de la RIPA, mais aussi conservées, d'une manière jugée licite et proportionnée au regard de ce mandat (paragraphes 58-60 ci-dessus). Pour que leur conservation ait été jugée licite, il fallait que ces communications aient correspondu soit à un « sélecteur fort » (lié aux requérantes ou à des personnes avec qui elles étaient en contact), soit à une « requête complexe ». De l'avis de la Cour, si certaines des communications des requérantes correspondaient à un « sélecteur fort » utilisé par le GCHQ, elles étaient aussi potentiellement exposées au risque d'être interceptées et conservées par la NSA dans le cadre du programme Upstream, au motif qu'elles étaient « à destination » ou « en provenance » d'un sélecteur relevant de l'article 702 de la FISA. Même si les communications des requérantes ne correspondaient pas à un sélecteur fort, certaines d'entre elles devaient néanmoins présenter un intérêt pour le renseignement. Avant avril 2017, ces communications avaient pu être interceptées et conservées dans le cadre du programme Upstream si elles étaient « en rapport » avec un sélecteur relevant de l'article 702. Dans cette hypothèse, les communications en question auraient pu se trouver encore en possession de la NSA à l'époque pertinente (c'est-à-dire au 7 novembre 2017), car celle-ci s'était bornée à indiquer que le changement de politique opéré en avril 2017 la conduirait à supprimer « dès que possible » les communications précédemment collectées sur Internet dans le cadre du programme Upstream (paragraphe 263 ci-dessus). Il s'ensuit que des communications « en

rapport » avec un sélecteur fort collectées avant cette époque pouvaient avoir été conservées quelque temps encore par la NSA.

470. Dans ces conditions, la Cour admet qu'à l'époque pertinente (c'est-à-dire au 7 novembre 2017), les requérantes des première et troisième affaires étaient potentiellement exposées au risque que certaines au moins de leurs communications aient été interceptées et conservées dans le cadre du programme Upstream.

471. Toutefois, les requérantes ne peuvent se voir reconnaître la qualité de victime du régime d'échange de renseignements que si elles étaient aussi potentiellement exposées au risque que leurs communications aient été demandées par le GCHQ, étant entendu que pareille demande supposait qu'un mandat visant à l'obtention des éléments recherchés ait déjà été émis. Or, comme la Cour l'a déjà indiqué, le fait que les communications d'au moins deux des requérantes de la troisième affaire aient été conservées par le GCHQ donne à penser que certaines au moins de leurs communications faisaient l'objet d'un mandat délivré en vertu de l'article 8 § 4 de la RIPA. La Cour admet donc que les requérantes des première et troisième affaires étaient aussi potentiellement exposées au risque que leurs communications aient été demandées par le GCHQ.

472. En conséquence, la Cour reconnaît aux requérantes des première et troisième affaires la qualité de victime en ce qui concerne leurs griefs relatifs au régime d'échange de renseignements. Dès lors, il y a lieu de rejeter l'exception préliminaire soulevée par le Gouvernement.

3. Sur le fond

a) L'arrêt de la chambre

473. Pour apprécier la conformité à l'article 8 du régime encadrant la réception d'éléments interceptés provenant de services de renseignement étrangers tels que la NSA, la chambre s'est fondée sur une version modifiée des six exigences minimales (paragraphe 275). Les deux premières exigences ne pouvant s'appliquer à la démarche consistant à demander à des gouvernements étrangers des éléments interceptés, la Cour a plutôt recherché si les circonstances dans lesquelles ces éléments pouvaient être demandés étaient circonscrites de manière suffisamment précise pour empêcher les États d'utiliser cette possibilité dans le but de contourner soit leur droit interne, soit leurs obligations conventionnelles. Elle a ensuite appliqué les quatre dernières exigences au traitement dont ces éléments faisaient l'objet une fois que les services de renseignement britanniques les avaient obtenus.

474. La chambre a jugé que la législation interne, assortie des précisions apportées par la modification du code de conduite en matière d'interception de communications, indiquait avec suffisamment de clarté la procédure à suivre pour demander à des services de renseignement étrangers soit une

interception, soit la transmission d'éléments interceptés. Elle a observé également que rien n'indiquait qu'il y ait eu des défaillances significatives dans l'application ou le fonctionnement de ce régime. Elle a donc conclu, à la majorité, qu'il n'y avait pas eu violation de l'article 8 de la Convention à cet égard.

b) Thèses des parties

475. Les requérantes estiment que les garanties encadrant le régime d'échange de renseignements étaient inadéquates. Elles soutiennent en particulier que les problèmes qui avaient conduit la chambre à conclure à la violation de l'article 8 de la Convention à raison du régime d'interception en masse – à savoir les lacunes de la supervision de l'utilisation des sélecteurs et le caractère inadéquat des garanties relatives aux données de communication associées – valaient tout autant pour le régime d'échange de renseignements.

476. Pour sa part, le Gouvernement avance que le régime d'échange de renseignements avait une base claire en droit interne puisqu'il découlait d'une loi complétée par le chapitre 12 du code de conduite en matière d'interception de communications, et que la loi en question était accessible. S'agissant de la prévisibilité, le Gouvernement avance qu'au lieu d'appliquer une version modifiée des six exigences minimales, la chambre aurait dû retenir le critère plus général – habituellement appliqué, selon lui, dans les affaires de collecte de renseignements ne mettant pas en cause des interceptions de communications – consistant à rechercher si la loi précisait l'étendue et les modalités d'exercice de tout pouvoir discrétionnaire avec suffisamment de clarté pour offrir au justiciable une protection adéquate contre les ingérences arbitraires. En tout état de cause, le Gouvernement estime que le régime d'échange de renseignements satisfaisait aux six exigences minimales. Selon lui, le code de conduite en matière d'interception de communications énonçait la nature des infractions susceptibles de donner lieu à la collecte de renseignements, il posait des limites à la durée d'exécution de cette mesure, et il décrivait les procédures à suivre pour l'examen, l'utilisation et la conservation des renseignements obtenus, ainsi que les circonstances dans lesquelles ceux-ci devaient être effacés ou détruits.

477. Enfin, le Gouvernement soutient qu'il n'existe aucune raison valable de distinguer les communications interceptées et les données de communication associées des autres types d'informations pouvant en principe être obtenues auprès des services de renseignement étrangers, par exemple des renseignements tirés de sources humaines infiltrées ou d'une surveillance audio/vidéo cachée. D'ailleurs, il est selon lui fréquent que les services de renseignements ne sachent même pas si les communications que leur fournissent leurs homologues étrangers sont le fruit d'une interception.

c) Observations des tiers intervenants

i. Le gouvernement français

478. Le gouvernement français souligne que l'échange de renseignements – ponctuel ou régulier – entre services alliés revêt une importance vitale, notamment contre les menaces diffuses et de plus en plus transnationales que les États doivent prévenir en se donnant pour objectif premier d'identifier des suspects avant qu'ils ne passent à l'acte. La lutte contre ces menaces justifie selon lui le développement d'une communauté du renseignement, sans laquelle les services ne pourraient pas accomplir les missions qui leur sont assignées, leurs moyens d'action étant limités à l'étranger.

479. En outre, le gouvernement français estime que dans le cadre de l'échange de renseignements, l'ingérence ne commence pas lors de l'interception mais lors de l'obtention des données, même si les renseignements en cause ont été interceptés à la demande de l'État destinataire. Prenant note de l'approche adoptée par la chambre aux fins de l'examen du régime d'échange de renseignements britannique, il invite la Grande Chambre à employer la même.

480. Le gouvernement français avance que la fiabilité du service récepteur est l'un des principaux critères retenus par l'État émetteur pour décider de l'opportunité d'un échange de données, raison pour laquelle l'État destinataire doit garantir la stricte confidentialité des informations qui lui sont communiquées. C'est pourquoi les garanties exigées pour le traitement des renseignements recueillis dans le cadre d'un échange de données avec un service allié devraient être conformes à la règle dite du « tiers service », qui interdirait à une agence ayant reçu des renseignements d'un service allié étranger de les communiquer à un tiers sans l'accord de ce service. En l'absence de cette assurance, les États pourraient refuser de transférer des renseignements.

ii. Le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression

481. Le rapporteur spécial estime que les règles applicables à l'acquisition de données auprès de services de renseignement étrangers devraient être identiques à celles qui régissent l'acquisition de données par les autorités internes elles-mêmes. Dans le cas contraire, les pouvoirs publics pourraient être conduits en pratique à externaliser leurs activités de surveillance en se soustrayant aux garanties offertes par le PIDCP.

iii. Access Now

482. Access Now avance qu'alors que les traités d'entraide judiciaire offrent un processus transparent et officiel permettant à un État partie de

demander des renseignements à un autre, le fonctionnement des programmes secrets de renseignements d'origine électromagnétique (par exemple, le réseau d'échange de renseignements Five Eyes, qui regroupe le Royaume-Uni, les États-Unis, l'Australie, le Canada et la Nouvelle-Zélande) est opaque et contraire aux normes internationales en matière de droits de l'homme. Ces programmes secrets ne seraient pas nécessaires, les renseignements pertinents pouvant être obtenus dans le cadre des traités d'entraide judiciaire.

iv. Dutch Against Plasterk (« Burgers tegen Plasterk »)

483. Dutch Against Plasterk, une coalition composée de cinq individus et de quatre associations, a engagé une procédure contre les Pays-Bas pour contester les échanges de données entre les autorités néerlandaises et les services de renseignement étrangers alliés (dont ceux des États-Unis et du Royaume-Uni).

484. Dans sa tierce intervention devant la Cour, cette coalition avance que l'échange de renseignements ne devrait être autorisé qu'accompagné de garanties suffisantes et à condition que l'autorité étrangère dispose d'une base légale solide pour l'interception de renseignements, à défaut de quoi il y aurait un risque de contournement de la protection apportée par l'article 8 de la Convention. Elle ajoute que les États ne devraient pas être autorisés à obtenir auprès d'autorités étrangères des éléments qu'ils ne peuvent pas légalement intercepter eux-mêmes.

v. Center for Democracy and Technology (« CDT ») et Pen American Center (« PEN America »)

485. CDT et PEN America avancent que les modalités de la coopération internationale en matière de données de masse et de surveillance des communications doivent satisfaire au minimum à trois conditions. Premièrement, les États devraient évaluer activement et vérifier la pertinence des mesures juridiques et administratives d'encadrement des interceptions mises en place par leurs alliés, et les mentionner dans leur droit interne. Deuxièmement, l'utilisation de sélecteurs propres à des cibles spécifiques visant à effectuer des recherches sur des éléments obtenus auprès de services étrangers alliés devrait être soumise à l'autorisation d'un organe indépendant, de préférence judiciaire, fondée sur l'existence de soupçons raisonnables. Troisièmement, les personnes ayant fait l'objet d'une surveillance devraient en être avisées *a posteriori*.

486. CDT et PEN America estiment que, contrairement aux exigences de l'article 8 de la Convention, les régimes d'interception mis en œuvre par la NSA – en particulier ceux qui découlent de l'article 702 de la FISA et du décret présidentiel n° 12333 – ne sont ni « prévus par la loi » ni

« proportionnés » au but poursuivi, et que ces lacunes affectent la légalité du régime d'échange de renseignements britannique.

vi. Le Réseau européen des institutions nationales des droits de l'homme (« le REINDH »)

487. Se fondant sur des exemples tirés des pratiques de certains États membres, le REINDH affirme que la nature des échanges internationaux de renseignements a considérablement évolué, si bien qu'il est désormais difficile de différencier les données dont l'interception a été demandée des données non sollicitées. Selon lui, les échanges internationaux de renseignements portaient initialement sur des transferts de données analysées (ou « renseignements finis »), mais l'apparition des nouvelles technologies a conduit à une augmentation des échanges de données « brutes » non analysées. Même lorsqu'il existe des accords encadrant la coopération bilatérale ou multilatérale en matière de renseignement, il serait devenu beaucoup plus difficile, du fait de l'avènement de l'automatisation et des mégadonnées, d'évaluer les éléments obtenus par une partie auprès de l'autre, et notamment de savoir s'ils demeurent dans les limites de la demande initiale. Cette situation appellerait la mise en place d'une supervision indépendante solide des échanges internationaux de renseignements, sans distinction entre les données demandées et les données non sollicitées. Les organes chargés de cette supervision devraient être légalement habilités à surveiller l'ensemble des activités de coopération internationale menées par les services de renseignement de leur ressort, à collaborer avec les organes de contrôle indépendants des États étrangers participant aux échanges de renseignements et, au besoin, à engager des experts indépendants spécialistes des technologies de l'information et de la communication modernes.

vii. Human Rights Watch (« HRW »)

488. HRW observe que les requêtes examinées en l'espèce portent essentiellement sur la réception de renseignements en provenance des États-Unis, mais elle pense que le réseau d'États au sein duquel des renseignements sur des communications sont échangés est bien plus vaste. Elle souligne que, par exemple, l'alliance « Five Eyes » comprend le Royaume-Uni, les États-Unis, l'Australie, le Canada et la Nouvelle-Zélande, mais qu'on pense qu'il existe aussi d'autres groupes d'échange de renseignements moins connus (par exemple, « Nine Eyes », qui, en plus des cinq pays précédents, compterait le Danemark, la France, les Pays-Bas et la Norvège ; « Fourteen Eyes », qui comprendrait les neuf pays de Nine Eyes plus l'Allemagne, la Belgique, l'Espagne, l'Italie et la Suède ; et « Forty-One Eyes », qui comprendrait les précédents plus d'autres pays de la coalition alliée en Afghanistan).

viii. Open Society Justice Initiative (« OSJI »)

489. OSJ estime que les États ne devraient ni recevoir de données émanant de tiers ni en demander en contournant les droits individuels protégés par l'article 8. Pour éviter que cela n'arrive, ils doivent selon elle mettre en place des garanties qui s'appliquent lors de la collecte initiale des éléments – notamment un contrôle préalable des antécédents de l'État étranger en matière de droits de l'homme et du droit et de la pratique de cet État en matière d'interception, ainsi qu'une supervision indépendante *a posteriori*, de préférence judiciaire, de toutes les modalités d'échange, afin de vérifier que des garanties existent et qu'elles sont appliquées.

ix. The Electronic Privacy Information Center (« EPIC »)

490. EPIC avance que la législation des États-Unis permet la surveillance massive et systématique des personnes non américaines dans le cadre de l'article 702 de la FISA et du décret présidentiel n° 12333. Selon elle, la surveillance mise en place aux États-Unis en application de l'article 702 repose sur l'assistance obligatoire des fournisseurs de services de communications et vise les personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis. Ce régime ne comporterait pas de contrôle *a priori* des activités de surveillance, il n'exigerait pas l'existence de soupçons raisonnables et n'imposerait aucune obligation légale d'information des personnes visées par une mesure de surveillance. L'examen annuel, par la FISC, des procédures de ciblage et de minimisation destinées à limiter la collecte de communications de ressortissants américains ou de personnes se trouvant aux États-Unis serait la seule obligation prévue par ce régime.

491. Le décret présidentiel n° 12333 autoriserait la NSA à collecter des renseignements et des contre-renseignements extérieurs. Il lui conférerait de larges pouvoirs pour mener des activités de surveillance d'informations d'origine électromagnétique provenant de sources très diverses, notamment les réseaux de fibres optiques. Ces informations seraient collectées hors du territoire des États-Unis. Aucun rapport ni aucune publication officielle ne ferait état de l'ampleur de la surveillance autorisée par ce décret, et celle-ci échapperait à tout contrôle juridictionnel.

492. EPIC estime que la surveillance exercée par la NSA n'est pas conforme à l'article 8 de la Convention parce que son champ d'application et sa durée ne sont pas limités, qu'elle ne fait pas l'objet d'un contrôle adéquat, que les personnes visées n'en sont pas informées et que les recours existants ne sont pas effectifs.

x. La Commission internationale de juristes

493. La Commission internationale de juristes porte à l'attention de la Cour les articles 15 et 16 des articles sur la responsabilité de l'État pour fait

internationalement illicite élaborés par la Commission du droit international (« les articles de la CDI »). Elle estime qu'un État contractant pourrait voir sa responsabilité engagée à raison de la surveillance massive réalisée par un État non contractant d'une part en vertu de l'article 15, si la coopération de l'un avec l'autre est organisée et structurée, et d'autre part en vertu de l'article 16 si l'État contractant a contribué au programme de surveillance alors qu'il savait ou aurait dû savoir que celui-ci était intrinsèquement contraire aux obligations internationales des États en matière de droits de l'homme. Selon elle, les États contractants qui participent ou contribuent à un programme de surveillance de masse sont tenus de mettre en place un système de garanties aux fins de la protection des droits découlant de l'article 8 de la Convention, et de protéger les personnes relevant de leur juridiction contre les violations de ces droits causées par des programmes de surveillance de masse.

xi. The Law Society of England and Wales

494. The Law Society of England and Wales considère que le régime découlant de l'article 8 § 4 de la RIPA et des codes correspondants n'offre pas de garanties solides ni transparentes en ce qui concerne les éléments relevant du secret professionnel des avocats. Les garanties applicables aux éléments relevant du secret professionnel obtenus par des États étrangers puis communiqués aux services de renseignement du Royaume-Uni étant identiques, elle estime que le régime d'échange de renseignements présente les mêmes lacunes.

d) Appréciation de la Cour

i. Le critère applicable

495. La chambre a jugé que l'interception de communications par des services de renseignement étrangers ne pouvait engager la responsabilité d'un État destinataire ni relever de la juridiction de celui-ci au sens de l'article 1 de la Convention, même si l'interception avait été réalisée à sa demande (voir le paragraphe 420 de l'arrêt de la chambre). En premier lieu, certains des tiers intervenants ayant invoqué les articles de la CDI, la chambre a estimé que ceux-ci n'auraient été pertinents que si les services de renseignement étrangers avaient été mis à la disposition de l'État destinataire et avaient agi dans l'exercice de prérogatives de puissance publique de celui-ci (article 6); ou si l'État destinataire avait aidé ou assisté les services de renseignement étrangers à intercepter les communications lorsque cela aurait constitué un fait internationalement illicite de la part de l'État responsable de ces services, que l'État destinataire en aurait eu connaissance et que l'interception aurait constitué un fait internationalement illicite si elle avait été faite par l'État destinataire (article 16), ou encore si

l'État destinataire avait donné des directives à l'État étranger ou exercé son contrôle sur celui-ci (article 17). En second lieu, du point de vue de la jurisprudence de la Cour, la chambre a relevé que l'interception de communications par des services de renseignement étrangers ne pouvait relever de la juridiction de l'État destinataire que si celui-ci exerçait son autorité ou son contrôle sur ces services (voir, par exemple, *Al-Skeini et autres c. Royaume-Uni* [GC], n° 55721/07, §§ 130-139, CEDH 2011, et *Jaloud c. Pays-Bas* [GC], n° 47708/08, §§ 139 et 151, CEDH 2014).

496. La Grande Chambre fait sienne la conclusion de la chambre selon laquelle aucune de ces hypothèses ne se vérifie en l'espèce, et elle relève d'ailleurs que les requérantes n'ont pas soutenu le contraire dans les observations qu'elles lui ont soumises. Dans ces conditions, à supposer qu'il y ait eu ingérence dans les droits garantis par l'article 8 de la Convention, cette ingérence n'a pu se produire qu'au stade de la demande initiale d'éléments interceptés et de leur réception ultérieure, de leur examen et de leur utilisation par les services de renseignement de l'État destinataire.

497. La protection accordée par la Convention se trouverait vidée de sa substance si les États pouvaient contourner leurs obligations conventionnelles en adressant à des États non contractants des demandes d'interception de communications ou de remise de communications interceptées, ou même – bien que cette éventualité ne soit pas directement en cause dans la présente affaire – obtenir ces communications par un accès direct aux bases de données de ces derniers. La Cour estime donc que les demandes d'éléments interceptés adressées aux États non contractants doivent avoir une base en droit interne, être accessibles à la personne concernée et prévisibles quant à leurs effets (*Roman Zakharov*, précité, § 228). L'échange de renseignements doit être encadré par des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités sont habilitées à formuler de telles demandes (*Roman Zakharov*, précité, § 229, *Malone*, précité, § 67, *Leander*, précité, § 51, *Huvig*, précité, § 29, *Kruslin*, précité, § 30, *Valenzuela Contreras*, précité, § 46, *Rotaru*, précité, § 55, *Weber et Saravia*, décision précitée, § 93, et *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 75) et offrant des garanties effectives contre l'utilisation de ce pouvoir à des fins de contournement du droit interne et/ou des obligations conventionnelles des États.

498. La Cour estime que dès la réception des éléments interceptés, l'État destinataire doit avoir mis en place des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction. Les garanties en question, qui ont d'abord été énoncées par la Cour dans sa jurisprudence relative à l'interception de communications par les États contractants, s'appliquent également à la réception, par un État contractant, d'éléments interceptés demandés à un

service de renseignement étranger. Dès lors, comme le soutient le Gouvernement, que les États ne sont pas toujours en mesure de savoir si des éléments reçus de services de renseignement étrangers sont le produit d'une interception, la Cour considère que les mêmes règles doivent s'appliquer à l'ensemble des éléments reçus de services de renseignement étrangers qui pourraient être le produit d'une interception.

499. Enfin, la Cour estime que tout régime autorisant des services de renseignements à demander à des États non contractants de procéder à une interception ou de leur transmettre des éléments interceptés doit être soumis à une supervision indépendante et doit également prévoir la possibilité d'un contrôle *a posteriori* indépendant.

ii. Application des critères susmentionnés au cas d'espèce

500. L'accord entre le Royaume-Uni et les États-Unis en matière de renseignement relatifs aux communications (*United Kingdom-United States Communications Intelligence Agreement*) du 5 mars 1946 autorise expressément l'échange d'éléments interceptés entre les États-Unis et le Royaume-Uni (paragraphe 103 ci-dessus). Toutefois, il a fallu attendre l'affaire *Liberty* (paragraphes 33-36 ci-dessus) pour que soient divulgués les détails des procédures internes (ou « non publiques ») mises en œuvre par les services de renseignement concernés. Par la suite, ces nouvelles informations ont été intégrées dans le chapitre 12 du code de conduite en matière d'interception de communications (paragraphe 116 ci-dessus) qui, comme indiqué précédemment, était un document public approuvé par les deux chambres du Parlement et dont devaient tenir compte les tribunaux et toutes les personnes exerçant des fonctions liées à l'interception de communications (paragraphes 93-94 ci-dessus). La Cour a admis que les dispositions en question pouvaient être prises en considération pour apprécier la prévisibilité du régime découlant de la RIPA (voir *Kennedy*, précité, § 157, et le paragraphe 366 ci-dessus), et il en va nécessairement de même pour le régime d'échange de renseignements.

501. En conséquence, la Cour considère que le régime de demande et de réception de renseignements émanant d'États non contractants avait une base claire en droit interne et qu'à la suite des modifications apportées au code de communication en matière d'interception de communications, ce droit était suffisamment accessible. Ledit régime poursuivant à n'en pas douter les buts légitimes de protection de la sécurité nationale, de défense de l'ordre et de prévention des infractions pénales, et de protection des droits et libertés d'autrui, la Cour, suivant sa méthodologie habituelle (paragraphe 334 ci-dessus), va maintenant examiner conjointement la prévisibilité et la nécessité du régime de partage de renseignements.

502. Le chapitre 12 du code de conduite en matière d'interception de communications (paragraphe 116 ci-dessus) suivait la même approche que les dispositions de la législation interne relatives à l'interception en masse.

Il énonçait que les services de renseignement britanniques ne pouvaient adresser à un gouvernement étranger une demande aux fins de l'obtention de communications interceptées non analysées et/ou de données de communication associées que si le ministre compétent avait déjà émis un mandat approprié en vertu de la RIPA, si l'assistance du gouvernement étranger était nécessaire pour obtenir les communications en question au motif que celles-ci ne pouvaient pas être obtenues dans le cadre de ce mandat (voir le paragraphe 12.2 du code de conduite, reproduit au paragraphe 116 ci-dessus) et si l'obtention de ces données était nécessaire et proportionnée au but visé. Le mandat d'interception émis en vertu de la RIPA exigé par ces dispositions était soit un mandat émis en vertu de l'article 8 § 1 à l'égard du sujet concerné, soit un mandat émis en vertu de l'article 8 § 4 accompagné d'un certificat comprenant une ou plusieurs « descriptions des éléments à intercepter » couvrant les communications du sujet ou, pour un individu dont on savait qu'il se trouvait dans les îles Britanniques, un mandat émis en vertu de l'article 8 § 4 accompagné, d'une part, d'un certificat comprenant une ou plusieurs « descriptions des éléments à intercepter » couvrant les communications de cet individu et, d'autre part, d'un document modificatif approprié établi conformément à l'article 16 § 3.

503. En cas de circonstances exceptionnelles, une demande de transmission de communications pouvait être faite sans qu'un mandat d'interception ait été émis à cet égard en vertu de la RIPA si cette demande ne constituait pas un contournement délibéré de la RIPA, si elle ne faisait pas autrement échec aux objectifs de cette loi (tel était le cas, par exemple, lorsqu'il n'était pas possible techniquement d'obtenir les communications en question au moyen d'une interception faite en vertu de la RIPA), et si l'obtention de ces communications par l'agence interceptrice était nécessaire et proportionnée au but visé. La demande devait alors être examinée et approuvée – le cas échéant – par le ministre lui-même et, en vertu de la version révisée du code de conduite en matière d'interception de communications, elle devait être signalée au Commissaire à l'interception des communications. Selon les informations divulguées dans le cadre de l'affaire *Liberty*, et confirmées dans les observations soumises à la chambre et à la Grande Chambre par le Gouvernement, il n'a jamais été fait de demande d'éléments interceptés sans qu'un mandat n'ait été émis en vertu de la RIPA (paragraphe 42 ci-dessus).

504. Au vu de ce qui précède, la Cour estime que le droit interne posait des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités étaient habilitées à demander des éléments interceptés à un État étranger.

505. Dans le cas où il existait déjà un mandat approprié délivré en vertu de l'article 8 § 1 ou de l'article 8 § 4 de la RIPA, ce mandat avait été autorisé par le ministre compétent. Plus précisément, il semble, au vu du

paragraphe 12.5 du code de conduite en matière d'interception de communications lu à la lumière de la note de bas de page qui l'accompagne, que lorsqu'une demande était fondée sur un mandat existant, elle visait à l'obtention de communications à destination ou en provenance de sélecteurs spécifiques (c'est-à-dire liées à un ou plusieurs individus spécifiques), ou en rapport avec de tels sélecteurs, et que le ministre compétent avait déjà approuvé la demande visant les communications de l'individu ou des individus concernés. Si, en cas de circonstances exceptionnelles, une demande de transmission de communications pouvait être faite sans qu'un mandat d'interception approprié ait été émis, cette demande devait être approuvée par le ministre lui-même et, si elle était liée à des sélecteurs spécifiques, celui-ci devait personnellement examiner et approuver l'examen de ces communications au regard de ces sélecteurs (paragraphe 116 ci-dessus).

506. Dès lors que l'approche suivie par législation interne à l'égard des demandes d'échange de renseignements était identique à celle applicable aux interceptions en masse et que le droit interne interdisait expressément le contournement de ses dispositions, il n'y a pas lieu pour la Cour d'examiner séparément la procédure d'autorisation.

507. S'agissant des garanties encadrant l'examen, l'utilisation, la conservation, la transmission à des tiers, l'effacement et la destruction des éléments interceptés demandés à un service de renseignement étranger, il ressort clairement du paragraphe 12.6 du code de conduite en matière d'interception de communications que lorsque les services de renseignement britanniques obtenaient auprès d'un État étranger des communications interceptées ou des données de communication associées qui se présentaient comme le produit d'une interception, celles-ci devaient être soumises aux mêmes règles et garanties internes que celles applicables aux contenus et données de même catégorie obtenus directement par les agences interceptrices dans le cadre d'une interception réalisée en vertu de la RIPA. Autrement dit, les garanties prévues par les articles 15 et 16 de la RIPA, complétées par les dispositions du code de conduite en matière d'interception de communications, s'appliquaient aussi aux communications et aux données de communication interceptées obtenues auprès de services de renseignement étrangers dès lors que celles-ci se « présentaient comme le produit d'une interception ».

508. Après examen des garanties prévues par les articles 15 et 16 de la RIPA pour le régime d'interception en masse, la Cour a estimé que les procédures applicables à la conservation des données obtenues, à l'accès à ces données, à leur examen, à leur utilisation, à leur transmission à des tiers, à leur effacement et à leur suppression étaient suffisamment claires et offraient une protection suffisante contre les abus (paragraphes 384-405 ci-dessus). S'appuyant sur les conclusions auxquelles elle est parvenue au paragraphe 498 ci-dessus, la Cour constate que le paragraphe 12.6 du code

de conduite en matière d'interception de communications n'étendait pas les garanties prévues par les articles 15 et 16 de la RIPA, complétées par les dispositions de ce code, à l'ensemble des éléments obtenus auprès de services de renseignement étrangers qui pouvaient être le produit d'une interception, car il limitait ces garanties aux éléments qui se présentaient comme le produit d'une interception. Toutefois, elle estime que cette circonstance ne rend pas à elle seule le régime d'échange de renseignements irrémédiablement contraire à l'article 8 de la Convention.

509. En ce qui concerne le régime découlant de l'article 8 § 4 de la RIPA, la Cour a exprimé des préoccupations quant à l'exclusion des données de communication associées de la garantie offerte par l'article 16. Or le régime institué par l'article 8 § 4 autorisait l'État à intercepter, à conserver et à examiner tous les paquets de communications acheminés par certains canaux de transmission. L'exclusion générale des données de communication de la garantie prévue par l'article 16 impliquait que même si elles ne présentaient pas d'intérêt pour le renseignement, l'ensemble de ces données pouvaient être examinées par les services de renseignement, apparemment sans restriction. En revanche, il ressort du chapitre 12 du code de conduite en matière d'interception de communications que les données de contenu et les données de communication associées n'étaient pas demandées en masse par les services de renseignement. Le paragraphe 12.5 de ce code et la note de bas de page qui l'accompagne énonçaient qu'une demande relevant d'un mandat existant visait à l'obtention de communications à destination ou en provenance de sélecteurs spécifiques (c'est-à-dire liées à des individus spécifiques), ou en rapport avec de tels sélecteurs, et que le ministre compétent devait déjà avoir approuvé la demande visant les communications de ces individus concernés. Si, en cas de circonstances exceptionnelles, une demande de transmission de communications pouvait être faite sans qu'un mandat d'interception ait été émis, cette demande devait être approuvée par le ministre lui-même et, si elle était liée à des sélecteurs spécifiques, celui-ci devait personnellement examiner et approuver l'examen de ces communications au regard de ces sélecteurs. Si la demande de transmission n'était pas liée à des sélecteurs spécifiques, les communications obtenues à la suite de cette demande ne pouvaient pas être examinées selon un facteur lié à un individu dont on savait qu'il se trouvait dans les îles Britanniques, sauf si le ministre avait approuvé l'examen de ces communications (paragraphe 116 ci-dessus). En d'autres termes, soit les demandes formulées par les services de renseignement concernaient les communications d'individus dont le ministre avait déjà jugé l'obtention nécessaire et proportionnée au but visé, soit les éléments obtenus étaient couverts par la garantie prévue à l'article 16 de la RIPA. Aucune demande de transmission d'éléments n'ayant été faite en l'absence d'un mandat, il semble qu'à ce jour, toutes les demandes aient relevé de la première catégorie.

510. Dans ces conditions, la Cour estime que les garanties mises en place au Royaume-Uni pour l'examen des données de contenu et des données de communication obtenues auprès de services de renseignement alliés, ainsi que pour l'utilisation, la conservation, la transmission à des tiers, l'effacement et la destruction de ces données étaient adéquates.

511. Enfin, la Cour observe que le Commissaire à l'interception des communications et l'IPT offraient un niveau de protection supplémentaire (paragraphe 41 ci-dessus). Le Commissaire avait pour mission de superviser le régime d'échanges de renseignements : toutes les demandes de transmission d'éléments faites en l'absence de mandat devaient lui être notifiées en vertu du paragraphe 12.7 du code de conduite en matière de communications (paragraphe 116 ci-dessus), et il supervisait par ailleurs la délivrance des mandats et la conservation des éléments par les services de renseignement.

512. Outre la supervision assurée par le Commissaire à l'interception des communications, l'IPT exerçait un contrôle *a posteriori* du régime d'échange de renseignements. Il ressort de l'affaire *Liberty* que quiconque souhaitait formuler un grief individuel ou général contre le régime d'échange de renseignements pouvait saisir l'IPT, et que celui-ci pouvait alors examiner les procédures tant « publiques » que « non publiques » pour apprécier la conformité de ce régime à la Convention.

513. En conséquence, la Cour estime que le régime de demande et de réception d'éléments interceptés était compatible avec l'article 8 de la Convention. Il existait des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités étaient habilitées à demander des éléments interceptés à un service de renseignement étranger, le droit interne comportait des garanties effectives contre l'utilisation de pareilles demandes à des fins de contournement de ses dispositions et/ou des obligations conventionnelles du Royaume-Uni, les garanties mises en place par le Royaume-Uni pour l'examen, l'utilisation, la conservation, la transmission à des tiers, l'effacement et la destruction des éléments en question étaient adéquates, et le régime en cause était soumis à la supervision indépendante du Commissaire à l'interception des communications et il pouvait faire l'objet d'un contrôle *a posteriori* exercé par l'IPT.

514. Partant, il n'y a pas eu violation de l'article 8 de la Convention à cet égard.

B. Sur l'article 10 de la Convention

515. Dans leur requête, les requérantes de la troisième affaire alléguaient en outre que le régime d'échange de renseignements emportait violation de leurs droits découlant de l'article 10 de la Convention. Dans la mesure où ce grief concernait les activités que les requérantes exerçaient en qualité

d'ONG, la chambre l'a déclaré irrecevable pour non-épuisement des voies de recours internes car les intéressées l'avaient soulevé trop tard dans la procédure interne pour qu'il pût être examiné (voir le paragraphe 473 de l'arrêt de la chambre). Il s'ensuit que cet aspect de la requête échappe à l'objet du litige soumis à l'examen de la Grande Chambre.

516. Les requérantes de la troisième affaire soutenaient également, de manière plus générale, que le régime d'échange de renseignements n'était pas conforme à l'article 10 de la Convention. Bien qu'elles aient formulé ce grief en temps utile devant l'IPT, la Cour fait sienne la conclusion de la chambre selon laquelle ce grief ne soulève aucune question distincte ou supplémentaire par rapport à celui fondé sur l'article 8 de la Convention (voir le paragraphe 474 de l'arrêt de la chambre). En conséquence, elle considère qu'il n'y a pas eu non plus violation de l'article 10 de la Convention à cet égard.

IV. SUR L'OBTENTION DE DONNÉES DE COMMUNICATION AUPRÈS DES FOURNISSEURS DE SERVICES DE COMMUNICATION

A. Sur l'article 8 of the Convention

517. Les requérantes de la deuxième affaire soutiennent que le régime d'acquisition de données de communication découlant du chapitre II de la RIPA était incompatible avec les droits que leur garantit l'article 8 de la Convention.

1. L'arrêt de la chambre

518. Au moment où la chambre a examiné l'affaire, le gouvernement britannique était en train de remplacer le cadre légal encadrant les activités de surveillance secrète par une nouvelle loi sur les pouvoirs d'enquête. Les dispositions du nouveau texte relatives à la conservation de données de communication par les fournisseurs de services de communication ont fait l'objet d'un recours en justice introduit au niveau national par Liberty. Dans le cadre de cette procédure, le Gouvernement a admis que les dispositions litigieuses étaient incompatibles avec les exigences du droit de l'Union européenne. En conséquence, la *High Court* a jugé la partie 4 de la loi incompatible avec les droits fondamentaux protégés par le droit de l'Union européenne car, en matière de justice pénale, l'accès aux données conservées n'était pas limité au but de lutter contre les « infractions graves » et, de manière générale, l'accès aux données conservées n'était pas soumis au contrôle préalable d'un tribunal ou d'une instance administrative indépendante (paragraphe 190 ci-dessus).

519. Eu égard à la primauté du droit de l'Union sur le droit britannique et au fait que le Gouvernement avait reconnu, au cours de la procédure

interne, que les dispositions de la loi de 2016 sur les pouvoirs d'enquête relatives à la conservation de données de communication par les fournisseurs de services de communication étaient incompatibles avec le droit de l'Union, la chambre a estimé « clair » que le droit interne commandait que tout régime permettant aux autorités d'accéder aux données conservées par un fournisseur de services de communication limite cet accès au but de lutter contre les « infractions graves » et le soumette au contrôle préalable d'un tribunal ou d'une instance administrative indépendante. Le premier régime présentant les mêmes « défauts » que son successeur, la chambre a conclu qu'il ne pouvait être considéré comme prévu par la loi au sens de l'article 8 de la Convention (voir les paragraphes 465-468 de l'arrêt de la chambre).

2. Thèses des parties

520. Les parties n'ont pas soumis de nouvelles observations sur ce grief devant la Grande Chambre.

3. Appréciation de la Cour

521. Le Gouvernement ne conteste pas les conclusions de la chambre devant la Grande Chambre, et celle-ci n'aperçoit aucune raison de s'en écarter.

522. Partant, la Cour estime qu'il y a eu en l'espèce violation de l'article 8 de la Convention au motif que le fonctionnement du régime découlant du chapitre II de la RIPA n'était pas « prévu par la loi ».

B. Article 10 de la Convention

523. Les requérantes de la deuxième affaire se plaignent aussi, sur le terrain de l'article 10 de la Convention, du régime d'acquisition de données de communication auprès des fournisseurs de services de communication.

1. L'arrêt de la chambre

524. La chambre a reconnu que le régime découlant du chapitre II de la RIPA offrait une protection renforcée lorsque l'accès à des données visait à identifier les sources d'un journaliste. En particulier, le paragraphe 3.77 du code de conduite sur l'acquisition de données de communication prévoyait que les demandes visant à déterminer la source d'une information journalistique devaient répondre à un impératif prépondérant d'intérêt public et respecter les procédures prévues par la loi de 1984 sur la police et les preuves en matière pénale (*Police and Criminal Evidence Act 1984*, « la PACE »), qui subordonne l'obtention de pareilles données à la saisine d'un tribunal en vue de la délivrance d'une injonction de produire. En vertu de l'Annexe 1 à la PACE, la demande d'injonction de produire doit être

adressée à un juge et donne lieu à une procédure contradictoire lorsqu'elle concerne des éléments totalement ou partiellement journalistiques. Le code de conduite sur l'acquisition de données de communication prévoyait également que l'on ne pouvait recourir à la procédure d'autorisation interne que si l'on estimait qu'une vie humaine était en péril imminent et qu'elle aurait risqué d'être mise en danger par le délai inhérent à la conduite d'une procédure d'autorisation judiciaire (voir le paragraphe 498 de l'arrêt de la chambre).

525. Toutefois, ces dispositions ne s'appliquaient qu'aux demandes visant à identifier la source d'un journaliste. Elles ne s'appliquaient pas à chacune des demandes visant les données de communication d'un journaliste ou susceptibles de conduire à une intrusion collatérale dans ces données de communication. De plus, il n'y avait pas de dispositions spéciales restreignant l'accès aux données de communication d'un journaliste au but de lutter contre les « infractions graves ». En conséquence, la chambre a estimé que ce régime ne pouvait être considéré comme « prévu par la loi » aux fins de l'examen du grief fondé sur l'article 10 (voir les paragraphes 496-499 de l'arrêt de la chambre).

2. Thèses des parties

526. Les parties n'ont pas soumis de nouvelles observations sur ce grief devant la Grande Chambre.

3. Appréciation de la Cour

527. Le Gouvernement ne conteste pas les conclusions de la chambre devant la Grande Chambre, et celle-ci n'aperçoit aucune raison de s'en écarter.

528. Partant, la Cour estime qu'il y a eu en l'espèce violation de l'article 10 de la Convention au motif que le fonctionnement du régime découlant du chapitre II de la RIPA n'était pas « prévu par la loi ».

V. SUR L'APPLICATION DE L'ARTICLE 41 DE LA CONVENTION

529. Aux termes de l'article 41 de la Convention,

> « Si la Cour déclare qu'il y a eu violation de la Convention ou de ses Protocoles, et si le droit interne de la Haute Partie contractante ne permet d'effacer qu'imparfaitement les conséquences de cette violation, la Cour accorde à la partie lésée, s'il y a lieu, une satisfaction équitable. »

A. Dommage

530. Les requérantes n'ont soumis aucune demande au titre du dommage matériel ou moral. Partant, la Cour considère qu'il n'y a pas lieu de leur octroyer de somme à cet égard.

B. Frais et dépens

531. Devant la chambre, les requérantes des première et deuxième affaires ont réclamé respectivement 208 958,55 livres sterling (GBP) et 45 127,89 GBP au titre des frais et dépens qu'elles disaient avoir engagés pour les besoins de la procédure. Les requérantes de la troisième affaire n'ont présenté aucune demande au titre des frais et dépens.

532. La chambre a octroyé au titre de la procédure menée devant elle 150 000 euros (EUR) aux requérantes de la première affaire, et 35 000 EUR aux requérantes de la deuxième affaire.

533. Devant la Grande Chambre, les requérantes de la première affaire réclament une somme supplémentaire de 138 036,66 GBP, les requérantes de la deuxième affaire une somme supplémentaire de 69 200,20 GBP, et les requérantes de la troisième affaire sollicitent 44 993,60 GBP.

534. Le Gouvernement conteste les montants réclamés.

535. Selon la jurisprudence de la Cour, un requérant ne peut obtenir le remboursement de ses frais et dépens que dans la mesure où se trouvent établis leur réalité, leur nécessité et le caractère raisonnable de leur taux. En l'espèce, compte tenu des documents dont elle dispose et des critères en question, la Cour juge raisonnable d'octroyer, au titre de la procédure suivie devant la chambre, 150 000 EUR aux requérantes de la première affaire et 35 000 EUR aux requérantes de la deuxième affaire, tous frais confondus. Au titre de la procédure suivie devant la Grande Chambre, la Cour juge également raisonnable d'octroyer les sommes suivantes, tous frais confondus : 77 500 EUR aux requérantes de la première affaire, 55 000 EUR aux requérantes de la deuxième affaire et 36 000 EUR aux requérantes de la troisième affaire.

C. Intérêts moratoires

536. La Cour juge approprié de calquer le taux des intérêts moratoires sur le taux d'intérêt de la facilité de prêt marginal de la Banque centrale européenne majoré de trois points de pourcentage.

PAR CES MOTIFS, LA COUR,

1. *Dit*, à l'unanimité, qu'il y a eu violation de l'article 8 de la Convention à raison du régime découlant de l'article 8 § 4 de la RIPA ;

2. *Dit*, à l'unanimité, qu'il y a eu violation de l'article 8 de la Convention à raison du régime découlant du chapitre II de la RIPA ;

3. *Dit*, par douze voix contre cinq, qu'il n'y a pas eu violation de l'article 8 de la Convention à raison de la réception de renseignements obtenus auprès de services de renseignement étrangers ;

4. *Dit*, à l'unanimité, que, dans la mesure où cette disposition était invoquée par les requérantes de la deuxième affaire, il y a eu violation de l'article 10 de la Convention à raison du régime découlant de l'article 8 § 4 de la RIPA et du régime découlant du chapitre II de cette loi ;

5. *Dit*, par douze voix contre cinq, qu'il n'y a pas eu violation de l'article 10 de la Convention à raison de la réception de renseignements obtenus auprès de services de renseignement étrangers ;

6. *Dit*, à l'unanimité,
   a) que l'État défendeur doit verser aux requérantes, dans un délai de trois mois, les sommes suivantes, à convertir dans la monnaie de l'État défendeur au taux applicable à la date du règlement :
      i. aux requérantes de la première affaire: 227 500 EUR (deux cent vingt-sept mille cinq cents euros), plus tout montant pouvant être dû par les requérantes sur cette somme à titre d'impôt, pour frais et dépens ;
      ii. aux requérantes de la deuxième affaire: 90 000 EUR (quatre-vingt-dix mille euros), plus tout montant pouvant être dû par les requérantes sur cette somme à titre d'impôt, pour frais et dépens ;
      iii. aux requérantes de la troisième affaire: 36 000 EUR (trente-six mille euros), plus tout montant pouvant être dû par les requérantes sur cette somme à titre d'impôt, pour frais et dépens ;
   b) qu'à compter de l'expiration dudit délai et jusqu'au versement, ces montants seront à majorer d'un intérêt simple à un taux égal à celui de la facilité de prêt marginal de la Banque centrale européenne applicable pendant cette période, augmenté de trois points de pourcentage ;

7. *Rejette*, à l'unanimité, le surplus de la demande de satisfaction équitable.

Fait en français et en anglais, puis prononcé en audience, le 25 mai 2021, en application de l'article 77 §§ 2 et 3 du règlement.

Søren Prebensen	Robert Spano
Adjoint à la greffière	Président

Au présent arrêt se trouve joint, conformément aux articles 45 § 2 de la Convention et 74 § 2 du règlement, l'exposé des opinions séparées suivantes :

– opinion en partie concordante commune aux juges Lemmens, Vehabović et Bošnjak ;
– opinion en partie concordante et en partie dissidente du juge Pinto de Albuquerque ;
– opinion en partie dissidente commune aux juges Lemmens, Vehabović, Ranzoni et Bošnjak.

R.S.O.
S.C.P.

OPINION EN PARTIE CONCORDANTE COMMUNE AUX JUGES LEMMENS, VEHABOVIĆ ET BOŠNJAK

(Traduction)

1. Nous souscrivons à toutes les conclusions auxquelles est parvenue la majorité dans le dispositif du présent arrêt, sauf en ce qui concerne les points 3 (non-violation de l'article 8 de la Convention à raison de la réception de renseignements obtenus auprès de services de renseignement étrangers) et 5 (non-violation de l'article 10 à raison de la réception de renseignements obtenus auprès de services de renseignement étrangers). Les raisons de notre désaccord avec ces conclusions sont exposées dans une opinion dissidente rédigée conjointement avec notre collègue le juge Ranzoni et jointe au présent arrêt. Dans la présente opinion, nous montrerons que si l'arrêt de la Cour est dans l'ensemble bien construit et formule un message assez clair, il manque une excellente occasion d'affirmer pleinement l'importance du droit au respect de la vie privée et de la correspondance face aux ingérences découlant de la surveillance de masse.

I. OBSERVATIONS LIMINAIRES

2. La présente affaire porte sur un exercice de mise en balance des intérêts légitimes des États contractants et de certains droits de l'homme et libertés fondamentales, notamment ceux protégés par l'article 8 de la Convention. En prélude à son appréciation (paragraphes 322 et 323 du présent arrêt), la Grande Chambre précise la nature des menaces contemporaines qui pèsent sur les États contractants et reconnaît combien l'interception en masse peut s'avérer utile pour les détecter et les prévenir. En outre, le présent arrêt souligne la nécessité du secret des opérations menées dans ce domaine et en reconnaît la légitimité, ce qui implique que peu d'informations sur le fonctionnement des systèmes d'interception sont rendues publiques, voire aucune. Si l'on peut souscrire, dans une certaine mesure, à cette analyse de l'intérêt légitime des États à recourir à l'interception en masse, cette introduction ne met pas autant l'accent sur l'importance de la vie privée ou de tout autre intérêt privé. Bien que cette circonstance n'ait pas d'incidence directe sur l'appréciation du système d'interception en masse ici en cause, il nous semble que le point de départ de l'examen de la Cour aurait dû être plus équilibré.

3. Avant de nous lancer dans l'analyse de ce qui nous paraît être les points faibles du présent arrêt, il nous semble important de rappeler que la vie privée est une condition préalable essentielle à un certain nombre d'intérêts individuels fondamentaux, et aussi à l'existence d'une société démocratique. Elle est indispensable au bien-être de la personne, à son

autonomie, à son épanouissement personnel et à sa capacité à développer des relations constructives avec autrui. Elle est aussi une condition sans laquelle l'individu ne peut jouir des droits civils, et donc de la qualité de membre libre et égal d'une société démocratique. Les ingérences dans le droit au respect la vie privée non seulement portent atteinte à l'autonomie individuelle et à la santé physique et mentale, mais constituent aussi un obstacle à l'auto-gouvernance démocratique.

4. En premier lieu, la vie privée est importante pour la santé mentale et physique de la personne. La simple sensation d'être constamment épié et jaugé par autrui peut avoir de graves conséquences sur la santé mentale et le bien-être physique. Placés dans une telle situation, les individus auront tendance à intérioriser à l'excès leur comportement social, ce qui les conduira à éprouver de la culpabilité ou de la honte au sujet des sentiments, des pensées, des désirs ou des pratiques qu'ils préfèrent garder pour eux. Ces tensions entre les exigences de la vie intérieure et les pressions liées à la présentation de soi peuvent être à l'origine de graves problèmes de santé.

5. En deuxième lieu, le regard externe et les pressions liées à la présentation de soi peuvent faire obstacle à « la promotion des libertés, de l'autonomie, de l'individualité, des rapports humains et au renforcement d'une société libre[1] ». La surveillance est paralysante en ce qu'elle réduit notre capacité à entrer spontanément et pleinement en relation avec autrui et à participer à certaines activités. Le manque d'intimité peut avoir un effet négatif sur notre vie intérieure, sur nos relations et, en définitive, sur notre autonomie. Ainsi « sera perdu (...) le noyau de l'intériorité personnelle, c'est-à-dire la source de l'esprit critique contre les convenances, de la créativité, de la rébellion et du renouvellement[2] ».

6. En troisième lieu, la vie privée est essentielle pour l'auto-gouvernance démocratique. La surveillance de masse exerce des pressions intérieures et extérieures incitant l'individu au conformisme, à la soumission et à l'obéissance. Elle risque d'être utilisée par l'État comme un moyen d'assurer l'obéissance et le conformisme tout en évitant l'oppression pure et simple et en se donnant un vernis de légitimité. Comme l'a écrit George Orwell dans son roman *1984*,

> « Il n'y a bien entendu pas moyen de savoir si l'on est observé à tel ou tel moment. À quelle fréquence et selon quel système la Mentopolice se branche sur un individu donné relève de la spéculation. Il n'est pas exclu qu'elle surveille tout le monde tout le temps. Une chose est sûre, elle peut se connecter sur chacun quand bon lui semble. Il faut donc vivre – et ainsi vit-on, l'habitude devenant une seconde nature – avec le présupposé que le moindre bruit sera surpris et le moindre geste – sauf dans le noir – scruté[3]. »

---

[1] Ruth Gavison (1980), « *Privacy and the Limits of Law* », Yale Law Journal 89, p. 347.

[2] Jeffrey Reiman (1995), « Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future », Santa Clara High Technology Law Journal 11:1, p. 42.

[3] George Orwell, *1984* (éditions Gallimard, 2018, traduit de l'anglais par Josée Kamoun),

7. En ménageant une sphère où l'activité humaine échappe aux regards, la vie privée favorise et encourage l'autonomie morale, condition *sine qua non* de l'auto-gouvernance dans les démocraties[4]. Seuls des êtres autonomes peuvent véritablement se gouverner eux-mêmes et jouir pleinement de tous les droits civils, tels que le droit de vote, les libertés d'association et de participation à la vie civile, les libertés de pensée, de conscience, de parole, d'expression et de religion, éléments essentiels de l'auto-gouvernance. Si notre liberté intérieure est compromise, on ne saurait dire que nous jouissons pleinement des libertés que ces droits sont censés nous apporter.

8. Mais la pression interne exercée sur la liberté n'est pas le seul effet de la surveillance. Dans la mesure où les citoyens conservent leur autonomie, la surveillance fait aussi peser des pressions externes sur leur liberté d'exercer leurs droits civils. De même que le fait de vivre sous un contrôle social constant risque de dissuader les citoyens d'agir selon leurs inclinations et leurs opinions par crainte de l'ostracisme, le fait de vivre sous une surveillance gouvernementale permanente risque de les inciter à se montrer un peu moins enclins à manifester leurs convictions politiques, à s'associer librement, à parler librement, à exprimer leurs divergences d'opinion et à se porter candidat aux fonctions publiques. Les effets cumulés d'inhibitions souvent mineures peuvent étouffer une société initialement libre, surtout si les individus sont éduqués dans un environnement gagné par le conformisme et la lâcheté morale. Dans l'opinion dissidente qu'il a jointe à l'arrêt *Osborn v. United States* rendu par la Cour suprême des États-Unis, le juge William O. Douglas a brillamment décrit la menace que la surveillance de masse fait peser sur nos libertés démocratiques :

> « (...) Le temps viendra peut-être où aucun de nous ne pourra être sûr que ses propos ne sont pas enregistrés pour un usage futur, où nous craindrons tous que nos pensées les plus secrètes nous échappent pour tomber entre les mains du gouvernement, où nos conversations les plus confidentielles et les plus intimes seront toujours à la merci d'oreilles avides et indiscrètes. Si cela arrive, notre vie privée et notre liberté disparaîtront. Si notre vie privée peut être violée à tout moment, comment pourrions-nous nous dire libres ? Si toutes nos paroles sont enregistrées et analysées, ou que nous craignons qu'elles le soient, comment pourrons-nous prétendre à la liberté d'expression ? Si chacune de nos relations est connue et enregistrée, si nos conversations avec nos relations sont interceptées, comment pourrons-nous prétendre à la liberté d'association ? Si cela arrive, nos concitoyens craindront d'exprimer autre chose que les pensées les plus prudentes et les plus orthodoxes et de s'associer avec quiconque, si ce n'est avec les personnes les plus respectables. La liberté, telle que la conçoit la Constitution, disparaîtra[5] ».

---

p. 13.

[4] Daniel Solove (2008), « *Understanding Privacy* » (Cambridge, MA: Harvard University Press), p. 98.

[5] *Osborn v. United States*, 385 U.S. 323 (1966).

9. En conclusion, le développement de nouvelles technologies qui permettent la surveillance de masse et l'utilisation optimale des informations collectées accroît les menaces contre la vie privée et le risque d'usage abusif de données à caractère personnel. Notre propos n'est pas de dire que ces menaces et risques se sont déjà largement concrétisés ou qu'ils ont déjà produit les conséquences décrites ci-dessus. Toutefois, pour élaborer un système propre à prévenir, à détecter et à réprimer les abus potentiels, il faut avoir clairement conscience de leur existence.

10. Nous estimons que ces considérations auraient dû conduire la Cour à accorder un poids nettement plus important à la vie privée en général – et à la confidentialité de la correspondance en particulier – lorsqu'elle les a mis en balance avec les intérêts légitimes de l'État défendeur à recourir à un régime d'interception en masse. Il s'ensuit que la Grande Chambre aurait dû a) identifier avec précision les atteintes à la vie privée et à la correspondance et leur accorder un poids suffisant, b) instaurer des garanties minimales claires propres à protéger les individus contre les atteintes arbitraires ou excessives, et c) en conséquence évaluer le régime d'interception en masse litigieux de manière plus rigoureuse.

II. LES INGÉRENCES DANS LA VIE PRIVÉE ET LA CORRESPONDANCE

11. Au paragraphe 325 du présent arrêt, la majorité détaille les différentes étapes du processus d'interception en masse. Elle considère que l'étape initiale, qu'elle définit comme l'interception et la rétention initiale des communications et des données de communication associées, « ne constitue pas une ingérence particulièrement importante » (paragraphe 330 de l'arrêt). Nous ne sommes pas de cet avis. À nos yeux, l'ingérence qui découle de cette étape initiale n'est pas anodine. D'abord parce que l'interception et la rétention initiale permettent aux autorités publiques d'entrer en possession de toutes les communications et données de communication associées d'un individu acheminées par des canaux de transmission sélectionnés. Ensuite parce que cette première étape est la condition *sine qua non* de la poursuite du processus, même s'il est vrai qu'à ce stade le contenu des communications n'est pas encore sélectionné ou porté à l'attention des responsables, et qu'aucune mesure ne peut donc être prise à l'encontre de tel ou tel individu. On ne sait pas quelle quantité exacte de communications et de données de communication associées est ainsi interceptée par les services de renseignement. Mais tout porte à croire qu'une bonne partie des communications de millions de personnes est régulièrement interceptée. Cette situation est aggravée par le fait qu'en règle générale, les individus concernés ignorent l'existence de cette ingérence. Lorsque ces individus ne peuvent pas savoir si leurs communications sont ciblées tout en ayant conscience que cette éventualité est très probable, ils

sont confrontés à une troisième forme d'ingérence en ce qu'ils risquent de modifier leur comportement en conséquence et d'en subir les sérieuses répercussions décrites aux paragraphes 3 à 8 ci-dessus.

12. Il ressort du paragraphe 330 du présent arrêt qu'une partie des communications interceptées est éliminée immédiatement. La Cour ne dispose d'aucune information sur la manière dont cette « élimination » s'opère. On peut raisonnablement supposer que cette opération n'est pas effectuée aléatoirement, sans logique interne, et que les services de renseignement utilisent à cet effet un certain nombre de critères destinés à séparer les éléments sans valeur des éléments potentiellement utiles. Le seul fait que cette opération soit réalisée de manière opaque et selon des critères inconnus est à notre avis très préoccupant. Un tel manque de transparence est à tout le moins difficilement compatible avec l'exigence de prévisibilité, qui est l'une des conditions de la licéité de toute ingérence dans les droits protégés par l'article 8 de la Convention. Or la majorité néglige totalement de se pencher sur cette étape particulière du processus d'interception en masse. Nous considérons qu'il s'agit là d'une importante lacune du présent arrêt.

III. LES GARANTIES MINIMALES DESTINÉES À PROTÉGER LES INDIVIDUS CONTRE LES INGÉRENCES ARBITRAIRES OU EXCESSIVES

13. Au paragraphe 335 du présent arrêt, la Cour donne un aperçu de sa jurisprudence sur six exigences minimales que le droit interne doit énoncer pour prévenir les abus de pouvoir dans le cadre d'interceptions de communications réalisées pour les besoins d'enquêtes pénales. Par ailleurs, elle précise avoir dit, dans l'arrêt *Roman Zakharov c. Russie* ([GC], nº 47143/06, CEDH 2015), que ces six garanties minimales s'appliquent aussi aux interceptions réalisées pour des raisons de sécurité nationale. La Grande Chambre souligne ensuite la nécessité de développer les critères en question et de les adapter aux particularités de l'interception en masse, puis elle énumère huit critères que les ordres juridiques nationaux doivent définir clairement pour satisfaire aux exigences de l'article 8 de la Convention (paragraphe 361 de l'arrêt).

14. Cette liste de critères est fort bien étayée, et elle constitue certainement un rempart contre l'arbitraire et les abus. Toutefois, les critères qui y figurent :

a) ne constituent pas véritablement des normes minimales autonomes car leur inobservation semble pouvoir être « rachetée » par un processus d'appréciation globale ;
b) exigent que le droit interne définisse clairement des garanties spécifiques, mais ne fixent pas eux-mêmes des garanties minimales ; et

c) n’offrent pas aux individus de protection matérielle explicite contre des ingérences disproportionnées, en particulier au stade de l’application des sélecteurs forts aux éléments collectés, et les garanties procédurales que ces critères renferment sont insuffisantes.

15. En ce qui concerne le point a), nous voudrions attirer l’attention du lecteur sur le paragraphe 360 du présent arrêt, où la Cour déclare qu’un régime d’interception en masse doit faire l’objet d’une appréciation globale. Si cette approche peut paraître attrayante, elle altère forcément la valeur de chacune des garanties. Pour notre part, nous estimons au contraire qu’une garantie qualifiée de minimale ne peut en aucun cas être contrebalancée par des facteurs compensateurs se rattachant à d’autres critères. Pour le dire autrement, le non-respect d’une garantie considérée comme minimale devrait automatiquement conduire à un constat de violation de l’article 8 de la Convention, quand bien même une appréciation globale pourrait donner un éclairage plus positif. Malheureusement, la majorité ne paraît pas avoir opté pour cette approche. Par ailleurs, il nous semble qu’une approche consistant à ériger des règles minimales en limites absolues, en lignes rouges intangibles et infranchissables, fournirait une protection plus solide et plus prévisible, ce qui est de la plus haute importance dans un domaine où les activités des autorités publiques demeurent hautement confidentielles, au point – selon les énonciations du présent arrêt (paragraphe 322) – que peu d’informations sur le fonctionnement du système sont rendues publiques, voire aucune, et que les informations mises à la disposition du public peuvent être formulées en termes abscons.

16. S’agissant du point b), la majorité déclare que les huit critères énumérés au paragraphe 361 doivent être clairement définis dans le cadre juridique national. Si cette exigence est louable, notamment du point de vue de la prévisibilité de la loi, les critères en question ne posent en eux-mêmes aucune exigence minimale, ni en ce qui concerne les conditions matérielles ou procédurales auxquelles le fonctionnement d’un régime d’interception en masse doit satisfaire ni en ce qui concerne le passage du stade initial du processus aux étapes plus intrusives. Cette lacune est en partie comblée par le fait que certains – mais pas la totalité – des éléments dont il est question aux paragraphes 348 à 360 de l’arrêt sont énoncés non seulement dans des passages descriptifs renvoyant à la jurisprudence existante, mais aussi sous une forme prescriptive posant certaines exigences, notamment en ce qui concerne les différents stades de l’autorisation de l’interception en masse. Toutefois, nous considérons que les exigences posées par la majorité ne vont pas assez loin dans la protection des individus contre les ingérences arbitraires, excessives ou abusives dans leur vie privée et leur correspondance.

17. Cela nous amène au point c). Pour ce qui est des interceptions ciblées, réalisées principalement à des fins de détection et d’investigation d’activités criminelles, la Cour a imposé un certain nombre de garanties

matérielles contre les abus. Par exemple, elle a exigé que la nature des infractions pouvant donner lieu à un mandat d'interception et les catégories de personnes dont les communications sont susceptibles d'être interceptées soient définies, et elle a fréquemment rappelé la nécessité d'un soupçon raisonnable. La majorité considère simplement que ces garanties ne sont pas aisément applicables à l'interception en masse. Si nous pouvons nous aussi convenir qu'elles ne sont pas directement transposables à l'interception en masse, la mise en place d'une protection matérielle solide n'en demeure pas moins indispensable. À cet égard, les garanties élaborées dans le cadre des interceptions ciblées visant à lutter contre la criminalité constituent une excellente source d'inspiration, comme nous nous efforcerons de l'expliquer ci-dessous.

18. Premièrement, à la différence de l'interception ciblée destinée à prévenir la criminalité, l'interception en masse est couramment utilisée à des fins de protection de la sécurité nationale. On voit mal pourquoi on ne pourrait pas exiger que les menaces potentielles contre la sécurité nationale et les circonstances dans lesquelles elles sont susceptibles de déclencher une interception en masse soient clairement définies dans la législation nationale.

19. En ce qui concerne la deuxième exigence matérielle à laquelle l'interception ciblée doit satisfaire, c'est-à-dire la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées, on peut admettre qu'une exigence analogue n'aurait guère de sens au stade initial de l'interception en masse, où toutes les communications acheminées par certains canaux de transmission sont interceptées de manière indiscriminée. Toutefois, l'ampleur d'une ingérence ne saurait justifier l'abandon d'une garantie particulière. En outre, aux stades ultérieurs de l'interception en masse, particulièrement lors de l'application de sélecteurs forts aux fins de la sélection et de l'analyse des communications d'un individu identifié, la situation devient largement comparable à celle de l'interception ciblée. Il ne serait pas excessif, mais au contraire tout à fait légitime, d'exiger que le cadre juridique définisse les catégories de personnes susceptibles d'être ciblées par l'application de sélecteurs forts.

20. En troisième lieu, l'exigence d'un soupçon raisonnable constitue une importante protection contre les atteintes arbitraires et disproportionnées à plusieurs droits conventionnels. Elle se rapporte à la probabilité qu'une infraction pénale s'analysant en une ingérence a été commise ou est sur le point de l'être. Si l'interception en masse ne devrait pas être utilisée à des fins d'investigation d'infractions, mais uniquement à des fins de protection de la sécurité nationale, nous estimons néanmoins que les motifs pour lesquels l'interception en masse peut être autorisée devraient être subordonnés à une exigence analogue à celle du soupçon raisonnable. Il en va particulièrement ainsi lorsqu'une interception en masse commence à cibler un individu identifié en utilisant des sélecteurs forts. Pour être clairs,

nous considérons que dans une société démocratique, les services de renseignement ne peuvent examiner les communications d'un individu et les données de communications associées que s'ils sont en mesure de prouver à un observateur objectif qu'il est possible que l'individu en question participe ou s'apprête à participer à des activités contraires à un intérêt de sécurité nationale bien précis, ou qu'il est en contact ou susceptible d'être en contact avec des individus qui participent ou s'apprêtent à participer à de telles activités. La majorité n'impose pas cette exigence ou une exigence analogue dans le présent arrêt.

21. En lieu et place de ces trois garanties, la majorité se borne à poser une exigence matérielle beaucoup trop générale en imposant que les motifs pour lesquels une interception en masse peut être autorisée et les circonstances dans lesquelles les communications d'un individu sont susceptibles d'être interceptées soient clairement définis dans le cadre juridique national. Malheureusement, les notions de « motifs » et de « circonstances » sont assez imprécises, d'autant qu'il n'en est donné aucune définition positive ou négative. En outre, il ressort des termes employés au paragraphe 361 de l'arrêt que l'exigence spécifique applicable aux motifs s'applique uniquement au stade de l'autorisation de l'interception en masse, et non aux étapes ultérieures, si bien qu'il n'existe aucun moyen de savoir si une quelconque exigence matérielle est applicable, par exemple, à l'application de sélecteurs forts ciblant les communications d'un individu identifié.

22. L'absence de protection matérielle adéquate entraîne d'importantes conséquences sur l'effectivité de la protection procédurale. L'exigence d'une autorisation préalable, que l'arrêt impose au stade initial de l'interception en masse et avant l'application de sélecteurs forts, est l'élément central de la protection procédurale. Toute autorisation préalable tend principalement à vérifier si l'ingérence envisagée respecte les critères matériels auxquels elle est subordonnée. Toutefois, si ces critères matériels sont vagues ou trop larges, ou s'ils font défaut, l'exigence d'une autorisation préalable ne saurait offrir une protection effective contre l'arbitraire et les abus.

23. L'arrêt exige que le stade initial de l'interception soit subordonné à une autorisation préalable et que celle-ci relève de la compétence d'un organe indépendant de l'exécutif. Nous souscrivons à cette idée. Toutefois, nous sommes en complet désaccord avec l'idée selon laquelle une autorisation préalable *interne* est à elle suffisante pour ce qui est de l'application de sélecteurs forts liés à des individus identifiables. Nous estimons au contraire qu'un contrôle judiciaire préalable est nécessaire à ce stade. Si la jurisprudence actuelle de la Cour n'exige pas nécessairement que l'interception ciblée de communications individuelles soit soumise à une autorisation judiciaire, nous estimons qu'un certain nombre de raisons militent en faveur d'un renforcement du niveau de protection s'agissant de

l'application de sélecteurs forts dans le cadre d'une interception en masse. Ces raisons sont les suivantes :

a) Contrairement à l'interception ciblée, l'interception en masse n'est pas circonscrite à une catégorie spécifique de personnes, si bien que le nombre de communications susceptibles d'être examinées est beaucoup plus élevé que dans le cas d'une interception ciblée ;

b) En outre, l'application d'un sélecteur fort lié à un individu identifié permet l'accès à un nombre beaucoup plus élevé de communications, notamment à celles où l'individu en question est mentionné, même s'il n'y a pas pris part (et non pas seulement aux communications échangées sur les outils de communication utilisés par l'individu lui-même) ;

c) Les interceptions ciblées réalisées à des fins de répression de la criminalité sont généralement soumises à une forme de contrôle judiciaire à un moment ou à un autre. Par exemple, la production de preuves obtenues au moyen d'une interception ciblée dans le cadre d'une procédurale pénale ultérieure donnera au tribunal saisi de cette procédure l'occasion de vérifier si l'interception en question était conforme aux exigences légales. Les interceptions en masse utilisant des sélecteurs forts ne donnent en général pas lieu à un tel contrôle judiciaire.

24. La majorité prend le contrepied de cette approche en considérant qu'une autorisation préalable interne est suffisante. Nous estimons pour notre part que le niveau de protection contre l'arbitraire et les abus conféré par une autorisation interne n'est pas comparable à celui qu'offre un contrôle indépendant. En particulier, on voit mal comment une personne ayant un lien organisationnel – voire collégial – avec l'organe dont émane la demande pourrait l'examiner en toute équité et objectivité. Les conditions de l'autorisation risquent alors de ne pas être pleinement respectées, ce qui ferait échec au but même de cette garantie. Ce risque est encore plus élevé en ce qui concerne les Hautes Parties contractantes qui n'ont pas de longue tradition de contrôle démocratique des services de renseignement.

25. Nous relevons que les gouvernements britannique et néerlandais ont soutenu que toute obligation d'expliquer ou de justifier les sélecteurs ou les critères de recherche dans l'autorisation restreindrait gravement l'effectivité de l'interception en masse (paragraphe 353 du présent arrêt), et que la majorité se montre assez réceptive à cet argument (paragraphe 354 du présent arrêt). Tel n'est pas notre cas. Nous pensons que dans une société démocratique, les communications et les données de communication associées d'un individu identifié ne doivent pas être ciblées et examinées sans son consentement, sauf s'il existe des raisons très convaincantes de le faire. Dès lors qu'un service de renseignement ou un autre organe n'est pas en mesure d'expliquer ces raisons et d'en démontrer la réalité devant une instance indépendante, il devrait tout simplement se voir refuser tout accès

aux communications en question. Nous reconnaissons que le processus ordinaire d'autorisation peut parfois s'avérer trop lourd pour neutraliser efficacement une menace dirigée contre la sécurité nationale, et qu'il est alors nécessaire de recourir à d'autres solutions. Toutefois, si un système d'autorisation solide destiné à protéger efficacement les droits de l'homme est perçu comme un obstacle inutile, la société démocratique doit en être avertie.

IV. APPRÉCIATION DU RÉGIME D'INTERCEPTION EN MASSE LITIGIEUX

26. Nous souscrivons aux conclusions auxquelles nos collègues de la Grande Chambre sont parvenus en ce qui concerne les points 1, 2 et 4 du dispositif de l'arrêt. Cela étant, nous estimons que l'examen de certains aspects du régime critiqué ne va pas assez loin et qu'il ne met pas suffisamment en évidence certaines de ses lacunes.

27. Par exemple, nous attirons l'attention du lecteur sur les motifs pour lesquels une interception en masse pouvait être autorisée dans le régime britannique alors en vigueur (paragraphes 368-371 de l'arrêt). Un mandat d'interception pouvait être délivré s'il s'avérait nécessaire a) dans l'intérêt de la sécurité nationale, b) aux fins de la prévention ou de la détection des infractions graves, ou c) aux fins de la sauvegarde de la prospérité économique du Royaume-Uni, dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale.

28. Les buts énumérés aux points a) et c) mentionnaient tous deux les intérêts de la sécurité nationale. Mais la sécurité nationale et ses intérêts n'étaient définis nulle part. Nous relevons que l'arrêt renvoie aux précisions données par le Commissaire à l'interception des communications quant à la manière dont la notion de sécurité nationale était conçue en pratique (paragraphe 369 de l'arrêt), mais nous estimons que ces précisions étaient insuffisantes au regard de l'exigence de prévisibilité. En outre, nous doutons que les précisions données par le Commissaire à l'interception des communications puissent être assimilées à une jurisprudence bien établie qui, selon celle de la Cour, peut compenser l'imprécision de la loi. En l'absence de définition claire, un individu ne pouvait savoir avec certitude, même en s'entourant de conseils éclairés, pour quels motifs précis ses communications étaient susceptibles d'être interceptées et analysées par les services de renseignement.

29. Le but mentionné au point b) ne présentait pas les mêmes défauts, exposés ci-dessus, que les buts énoncés aux points a) et c). L'infraction grave était définie comme étant une infraction dont l'auteur (âgé d'au moins vingt et un an et sans antécédents judiciaires) pouvait raisonnablement s'attendre à être condamné à une peine d'emprisonnement d'une durée égale ou supérieure à trois ans, ou une infraction constituée par un acte caractérisé

par l'usage de la violence, par un gain pécuniaire important ou par sa commission par une multiplicité de personnes poursuivant un objectif commun (paragraphe 369 de l'arrêt). Cette définition s'applique à des actes très divers, ce qui soulève des doutes sérieux quant à la proportionnalité de ce motif d'interception. En outre, dans une société démocratique, les services de renseignement ne devraient pas être habilités à lutter contre la criminalité, sauf lorsqu'elle menace la sécurité nationale[6]. Les explications du Gouvernement selon lesquelles les informations obtenues au moyen d'une interception en masse ne pouvaient être utilisées dans le cadre de poursuites pénales ne nous convainquent pas. Il apparaît au contraire que les forces de l'ordre peuvent agir sur la base d'informations obtenues de cette manière, notamment en procédant à des mesures d'instruction ou même à des arrestations, qui aboutiront à leur tour à des preuves utilisables à des fins de poursuite. Il est probable que dans un avenir proche, ce motif sera utilisé pour faire sortir les enquêtes criminelles du domaine de la surveillance ciblée et les faire rentrer dans celui de l'interception en masse.

V. CONCLUSION

30. Il est rare que la Cour ait à trancher une affaire déterminante pour l'avenir de nos sociétés. La présente affaire en est un exemple. La Grande Chambre a partiellement saisi l'occasion qui lui était offerte en établissant un ensemble complet de principes destinés à protéger les droits de l'homme et les libertés fondamentales, notamment ceux consacrés par les articles 8 et 10 de la Convention. Toutefois, comme nous l'avons expliqué dans la présente opinion séparée, lorsqu'elle a effectué l'exercice de mise en balance, la majorité n'a pas accordé un poids suffisant au droit au respect de la vie privée et de la correspondance, qui demeure à certains égards insuffisamment protégé contre les atteintes susceptibles de découler de l'interception en masse. Il est permis d'espérer qu'à l'occasion de futures affaires soulevant des questions d'ingérence concrète dans les droits d'individus spécifiques, la Cour interprétera et précisera ces principes de manière à protéger comme il se doit la société démocratique et les valeurs qu'elle défend.

[6] Voir, par exemple, la recommandation 1402 (1999) de l'Assemblée parlementaire du Conseil de l'Europe sur le contrôle des services de sécurité intérieure dans les États membres du Conseil de l'Europe, et en particulier la ligne directrice A ii). Si cette recommandation porte sur les activités des services de sécurité intérieure, nous estimons qu'elle est parfaitement susceptible de s'appliquer également aux activités de renseignement extérieur.

OPINION EN PARTIE CONCORDANTE ET EN PARTIE DISSIDENTE DU JUGE PINTO DE ALBUQUERQUE

(Traduction)

I. INTRODUCTION

1. J'ai voté avec la majorité, sauf en ce qui concerne son constat de non-violation des articles 8 et 10 à raison de la réception d'éléments interceptés provenant de services de renseignement étrangers, c'est-à-dire les données de masse interceptées par l'Office national de sécurité américain (*National Security Agency*, « la NSA ») dans le cadre des programmes PRISM et Upstream. Par ailleurs, je marque mon désaccord avec les bases du raisonnement qui conduit la majorité à conclure à la violation des articles 8 et 10. La présente opinion vise à exposer les raisons de mon désaccord[1].

II. DÉCONSTRUCTION DU RÉGIME D'INTERCEPTION EN MASSE *PRO AUTORITATE* DE LA COUR

A. Un langage imprécis

2. Je tiens à dire d'emblée, et je le regrette, que le langage employé par la Cour est d'une imprécision inadmissible, ce que je démontrerai dans la présente opinion. S'il arrive parfois à la Cour d'employer délibérément un langage imprécis pour laisser à l'État défendeur une certaine latitude aux fins de l'exécution du présent arrêt, cette imprécision traduit en d'autres occasions l'hésitation des juges à accomplir leur fonction juridictionnelle. Cette attitude affaiblit l'autorité de la Cour et altère la valeur normative du présent arrêt.

3. Dès lors que les notions juridiques du droit européen des droits de l'homme sont autonomes, en ce qu'elles ne sont pas strictement dépendantes du sens et de la portée de celles qui leur correspondent dans les ordres juridiques nationaux, et que l'affaire dont la Grande Chambre était saisie soulevait des questions de droit nouvelles, la Cour aurait dû fixer noir sur blanc le sens des notions juridiques fondamentales qu'elle utilise dans le présent arrêt[2], indépendamment du sens que leur donnaient la loi de 2000 portant réglementation des pouvoirs d'enquête (*Regulation of Investigatory Powers Act 2000*, « la RIPA »), le code de conduite en matière d'interception de communications (*Interception of Communications Code of Practice*, « le code de conduite ») et les « procédures non publiques ». Dans un souci de clarté conceptuelle, je donnerai aux termes énumérés ci-après les définitions suivantes :

> **a) « sujets d'interception »** : les personnes physiques ou morales – notamment les services publics, les sociétés privées, les ONG et les organisations de la société civile – dont les communications peuvent être ou sont interceptées[3] ;
>
> **b) « données interceptées » ou « données de masse »** : le contenu des communications électroniques et les données de communication associées collectées au moyen d'une interception en masse[4] ;

---

[1] C'est la deuxième fois que je formule une opinion séparée au sujet de l'interception en masse. Dans l'affaire *Szábo et Vissy c. Hongrie*, n° 37138/14, 12 janvier 2016, j'ai exprimé mon opinion sur la voie dangereuse dans laquelle le régime hongrois de l'interception en masse s'était engagé et sur les conséquences fâcheuses auxquelles elle aboutirait. Les discussions qui se sont tenues devant la Grande Chambre et une mise en balance soigneuse des arguments en présence ne m'ont pas fait dévier d'un iota de ma position antérieure. Au contraire, je suis plus que jamais convaincu que ce que j'ai écrit en 2016 est encore tout à fait d'actualité, malheureusement. La présente opinion doit donc être lue en parallèle avec ce que j'ai écrit il y a cinq ans.

[2] On trouvera un exemple de cette bonne pratique dans l'arrêt *Rohlena c. République tchèque* [GC], n° 59552/08, 27 janvier 2015.

[3] La notion employée par le droit interne était analogue, voir l'article 20 de la RIPA.

[4] La notion employée par le droit interne était différente, voir l'article 20 de la RIPA.

c) « données de communication associées » : les données nécessaires à la localisation de la source d'une communication électronique et de sa destination, à la détermination de la date, de l'heure, de la durée et du type de communication, à l'identification de l'équipement de communication utilisé et à la localisation des terminaux d'équipement et de communication. Il s'agit notamment du nom et de l'adresse de l'utilisateur, des numéros de téléphone de l'appelant et de l'appelé et des adresses IP des services Internet[5] ;

d) « interception en masse » : interception ciblée ou non ciblée de communications électroniques (et des données de communication associées) acheminées par des canaux de transmission réalisée au moyen de sélecteurs forts et de sélecteurs ;

e) « canaux de transmission » : dispositifs d'acheminement de communications électroniques (principalement des câbles sous-marins composés de fibres optiques) ;

f) « sélecteurs forts » : identifieurs spécifiques (individuels) liés à une cible identifiée ou identifiable qui permettent de collecter des communications à destination ou en provenance de cette cible ou en rapport avec celle-ci ;

g) « sélecteurs » : identifieurs non spécifiques (non individuels) ;

h) communication « à destination » ou « en provenance » d'une cible : communication électronique dont l'expéditeur ou le destinataire utilise le sélecteur ciblé ;

i) communication « en rapport » avec une cible : communication électronique interceptée dans laquelle figure le sélecteur ciblé mais à laquelle la cible n'a pas forcément participé ;

j) « communication extérieure » : communication envoyée ou reçue hors du territoire national[6] ;

k) « communication » : « mots, musique, sons, images visuelles ou données de toute nature et signaux visant à transmettre quelque chose entre des personnes, entre une personne et un objet, ou entre des objets, ou encore à activer ou contrôler un appareil quelconque[7] » ;

l) « procédures non publiques » : règles et pratiques internes secrètes d'une autorité interceptrice.

B. Une méthodologie biaisée

4. L'approche méthodologique adoptée par la Cour dans la présente affaire est regrettable, pour deux raisons essentielles. En premier lieu, la Cour n'hésite pas à trancher une affaire de cette importance « en ne disposant que d'informations limitées sur la manière dont [les régimes encadrant dans les États contractants l'interception en masse] fonctionnent[8]

[5] La notion employée par le droit interne était plus restreinte, voir l'article 20 de la RIPA. L'article 21 §§ 4, 6 et 7 de ce texte employait la notion de « données de communication ».
[6] Cette notion est analogue à celle employée par l'article 20 de la RIPA.
[7] Cette définition, qui figurait dans l'article 81 de la RIPA, peut aussi être employée par la Cour.
[8] Paragraphe 323 du présent arrêt.

». Par exemple, bien que le Gouvernement n'ait fourni aucune indication sur la nature et le degré de précision des sélecteurs utilisés par ses services, ni sur le nombre de canaux de transmission interceptés, ni sur les modalités du choix des canaux de transmission, ni sur la nature des rapports de renseignement élaborés au sujet des données de communication associées, la Cour n'a pas insisté pour obtenir ces informations cruciales. Le Tribunal des pouvoirs d'enquête (*Investigatory Powers Tribunal*, « l'IPT ») a examiné les « procédures non publiques[9] », le Commissaire à l'interception des communications (*Interception of Communications Commissioner*) a eu accès aux « éléments confidentiels[10] », et même le contrôleur indépendant de la législation sur le terrorisme (*Independent Reviewer of Terrorism Legislation*) a pris connaissance de « nombreux éléments confidentiels[11] », mais la Cour n'a pas examiné ces éléments, et elle ne le pouvait pas. Il est manifeste que la Cour manquait d'éléments suffisamment circonstanciés pour procéder à une analyse et à un examen structurels complets de l'interception en masse pratiquée au Royaume-Uni. Il est regrettable qu'elle n'ait invoqué le caractère extrêmement sensible de l'objet de la présente affaire, qu'elle a souligné à plusieurs reprises, que pour insister sur la nécessité de « l'effectivité[12] » et de la « flexibilité[13] » du système d'interception en masse, et non pour recueillir l'ensemble des preuves dont elle avait besoin pour rendre un arrêt factuellement étayé. Cette autolimitation du pouvoir reconnu à la Cour dans le domaine de la recherche des preuves montre que les juges de Strasbourg ne considèrent pas la Cour comme un véritable organe juridictionnel ayant le pouvoir d'enjoindre aux parties de lui accorder un accès illimité et inconditionnel aux preuves pertinentes pour l'objet de l'affaire. La Cour en est réduite à formuler des « suppositions éclairées » sur l'intensité prévisible de l'ingérence dans les droits individuels découlant des différentes étapes du processus d'interception. Mais il est problématique d'élaborer des normes fondées sur des « suppositions éclairées », car ces normes refléteront les idées reçues et les partis pris du régulateur, qui sont ici flagrants. L'argumentation du Gouvernement se résume à cette simple injonction : « faites-nous confiance ». La majorité se résout à y obtempérer, au risque de favoriser la collecte excessive d'informations. Pour ma part, je ne m'y résous pas. Comme l'a déclaré le Comité du président des États-Unis pour l'examen des technologies de renseignement et de communication (*United States Presidential Review Board*), « les Américains ne doivent pas commettre l'erreur de faire confiance aux autorités[14] ». Les Européens non plus.

---

[9] Paragraphes 33 et 50 du présent arrêt.
[10] Paragraphe 136 du présent arrêt.
[11] Paragraphe 424 du présent arrêt.
[12] Paragraphe 353 du présent arrêt.
[13] Paragraphe 354 du présent arrêt.
[14] *« Liberty and Security in a Changing World, Report and Recommendations of the*

5. En second lieu, cette autolimitation que la Cour s'impose en matière probatoire et juridictionnelle la conduit à tenir pour acquis que l'interception en masse est inévitable, et plus encore sous la forme d'un régime d'interception généralisée, non ciblée et visant les communications de personnes sur lesquelles ne pèse aucun soupçon, tel que le souhaitaient l'État défendeur et les tiers intervenants dans la présente affaire et l'affaire *Centrum för rättvisa c. Suède*[15]. Le Gouvernement tient un raisonnement circulaire consistant à affirmer que l'interception en masse était incompatible avec l'exigence d'un soupçon raisonnable parce qu'elle était par définition non ciblée, et qu'elle était non ciblée parce qu'elle n'était pas subordonnée à l'existence de soupçons raisonnables[16]. La Cour emboîte le pas au Gouvernement en reprenant la thèse de celui-ci dans une formule péremptoire :

> « l'exigence d'un « soupçon raisonnable », que l'on trouve dans la jurisprudence de la Cour relative aux interceptions ciblées pratiquées dans le cadre d'une enquête pénale, est moins pertinente dans le contexte des interceptions en masse, qui ont en principe un but préventif, que dans le contexte d'une enquête portant sur une cible précise et/ou une infraction identifiable[17]. »

Ce nouveau paradigme implique que la Cour s'écarte de la jurisprudence établie selon laquelle 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[18] ». La Cour avait déjà évalué les systèmes d'interception allemand et britannique au regard d'un critère exactement identique à celui applicable à l'interception ciblée : je me réfère ici à la surveillance stratégique généralisée mise en place par la loi G10 en cause dans l'affaire *Weber et Saravia c. Allemagne*[19], à la collecte systématique des

---

President's Review Group on Intelligence and Communications Technologies », 12 décembre 2013, p. 114.

[15] *Centrum för rättvisa c. Suède*, (n° 35252/08), rendu le même jour que le présent arrêt. On relèvera que les observations des gouvernements français, néerlandais et norvégien portaient précisément sur ce point : selon eux, rien ne justifiait que soit ajouté aux régimes d'interception de masse un critère tiré de la nécessité d'un « soupçon raisonnable (paragraphes 301, 305 et 309 du présent arrêt).

[16] Voir la plaidoirie du gouvernement défendeur à l'audience tenue devant la Grande Chambre le 10 juillet 2019 « [le critère tiré de la nécessité d'un soupçon raisonnable et l'exigence d'une notification *a posteriori*] sont fondamentalement incompatibles avec le fonctionnement d'un régime qui n'est pas fondé sur l'existence de cibles de surveillance précisément définies. Le régime découlant de l'article 8 § 4 est par nature non ciblé. Il sert à découvrir des menaces inconnues contre la sécurité nationale ou de crime. La nécessité de soupçons raisonnables n'y a donc absolument pas sa place. Pareille exigence affecterait son utilité (…) ». En fin de compte, cette thèse se résume donc à la question de « l'utilité » d'un régime d'interception en masse visant les communications de personnes sur lesquelles ne pèse aucun soupçon.

[17] Paragraphe 348 du présent arrêt.

[18] *Liberty et autres c. Royaume-Uni* n° 58243/00, § 63, 1er juillet 2008.

télécommunications envoyés ou reçues hors des îles Britanniques mise en place par la loi de 1985 sur les interceptions de communications (*Interception of Communications Act 1985*) qui était en cause dans l'affaire *Liberty et autres c. Royaume-Uni*[20], et à l'interception de gros volumes de communications intérieures autorisée par la loi de 2000 portant réglementation des pouvoirs d'enquête (*Regulation of Investigatory Powers Act 2000*) en cause dans l'affaire *Kennedy c. Royaume-Uni*[21]. La Cour s'écarte sans bonne raison des principes de cette jurisprudence, comme je le montrerai ci-dessous.

6. En outre, la Cour n'accorde pas suffisamment de poids au fait qu'elle avait reformulé et effectivement appliqué sa jurisprudence antérieure dans trois affaires récentes, dont l'une portait indirectement – et les deux autres directement – sur l'interception non ciblée de communications. Je me réfère au affaires *Roman Zakharov c.* Russie[22], *Szábo et Vissy c. Hongrie*[23] et *Mustafa Sezgin Tanrıkulu c. Turquie*[24]. Il est révélateur que la Cour ait aussi fait usage, dans l'arrêt *Roman Zakharov c. Russie*[25], des critères *Weber et Saravia* pour apprécier des mesures opérationnelles d'investigation qui visaient notamment des communications postales et télégraphiques et pouvaient s'appliquer à « tout usager de services de téléphonie mobile[26] » aux fins de la protection de la sécurité nationale, militaire, économique ou écologique[27]. Dans cette affaire, la Grande Chambre est allée jusqu'à critiquer la pratique des tribunaux qui consistait à délivrer « une autorisation qui ne mentionn[ait] pas une personne précise ou un numéro de téléphone particulier à placer sur écoute, mais autoris[ait] l'interception de toutes les communications téléphoniques dans le secteur où une infraction pénale [avait] été commise[28] ». Dans l'arrêt *Szábo et Vissy c. Hongrie*[29], la Cour a été encore plus explicite en censurant « la surveillance illimitée d'un grand nombre de citoyens[30] » qui visait à lutter contre le terrorisme et à venir au secours de ressortissants hongrois en détresse à l'étranger[31]. Si elle a admis la nécessité de l'interception en masse à des fins de lutte contre les menaces tant intérieures qu'extérieures, la Cour a subordonné toute mesure de

---

[19] *Weber et Saravia c. Allemagne* (déc.), n° 54934/00, §§ 95 et 114, CEDH 2006-XI.
[20] *Liberty et autres*, précité, §§ 63-65.
[21] *Kennedy c. Royaume-Uni*, n° 26839/05, §§ 158-160, 18 mai 2010.
[22] *Roman Zakharov c. Russie* [GC], n° 47143/06, §§ 231 et 264, CEDH 2015.
[23] *Szábo et Vissy*, précité.
[24] *Mustafa Sezgin Tanrıkulu c. Turquie*, n° 27473/06, 18 juillet 2017.
[25] *Roman Zakharov*, précité, §§ 231 et 264.
[26] *Ibidem*, §§ 175-178.
[27] *Ibidem*, §§ 31, 246-248.
[28] *Ibidem*, § 265. Les autorisations de « surveillance de zone » constituent sans conteste une source potentielle d'interception en masse.
[29] *Szábo et Vissy*, précité.
[30] *Ibidem*, § 67.
[31] *Ibidem*, § 63.

surveillance à l'existence d'« un soupçon à l'égard de la personne visée[32] », en application des critères *Weber et Saravia*[33]. Dans l'affaire ultérieure *Mustafa Sezgin Tanrıkulu c. Turquie*[34], après avoir rappelé et confirmé la jurisprudence *Weber et Saravia*, *Roman Zakharov* et *Szábo et Vissy*, la Cour a critiqué une décision d'une juridiction interne qui autorisait, à des fins de prévention d'actes criminels par des organisations terroristes, l'interception des communications téléphoniques et électroniques de toute personne présente en Turquie.

7. En l'espèce, la Cour déclare que « ces deux affaires [*Liberty et autres* et *Weber et Saravia*] remontent à plus de dix ans » et que l'étendue de l'activité de surveillance examinée dans ces deux affaires était « bien plus restreinte[35] », puis elle justifie l'abandon de sa jurisprudence antérieure[36] par trois arguments factuellement erronés.

8. Son premier argument consiste à dire que le « but déclaré » de l'interception en masse consiste « dans bien des cas » à contrôler des communications échangées par des personnes se trouvant hors de la compétence territoriale de l'État et « qui ne peuvent être contrôlées par d'autres formes de surveillance[37] ». La Cour ne fournit aucune preuve – elle ne le pouvait pas – de ce que le « but déclaré » de l'interception en masse, sans parler de la manière dont elle était utilisée en pratique, se limitait « dans bien des cas » à viser des personnes se trouvant hors de la compétence territoriale de l'État. Au contraire, tous les documents disponibles faisant autorité sur l'interception en masse, que la Cour choisit d'ignorer, témoignent d'une tout autre réalité. Compte tenu de l'insuffisance des preuves fournies par le gouvernement défendeur, il est incompréhensible que la Cour fasse fi des constats opérés par le Conseil de l'Europe et l'Union européenne, qui ont été divulgués au public dans une pléthore de documents faisant autorité sur l'interception en masse publiés après le scandale suscité par les révélations d'Edward Snowden. Je renvoie notamment aux résolutions 1954 (2013) et 2045 (2015) et à la recommandation 2067 (2015) de l'Assemblée parlementaire du Conseil de l'Europe, à la déclaration adoptée le 11 juin 2013 par le Comité des Ministres et à la réponse de celui-ci à la recommandation 2067 (2015) de la PACE, à la recommandation de politique générale n° 11 de la Commission européenne contre le racisme et l'intolérance, aux observations formulées par le Commissaire aux droits de l'homme le 24 octobre 2013, à ses documents thématiques du 8 décembre 2014 et de mai 2015 et à son rapport

---

[32] *Ibidem*, § 71.
[33] *Ibidem*, § 56.
[34] *Mustafa Sezgin Tanrıkulu*, précité, §§ 56 et 57.
[35] Paragraphe 341 du présent arrêt. Cette assertion méconnaît les arrêts *Roman Zakharov* et *Szábo et Vissy*, précités.
[36] Paragraphes 344-346 du présent arrêt.
[37] Paragraphe 344 du présent arrêt.

du 1er octobre 2015 sur les lacunes de la supervision des services de renseignement et de sécurité allemands, aux résolutions adoptées par le Parlement européen le 12 mars 2014 et le 29 octobre 2015, à l'avis émis le 20 février 2014 par le Contrôleur européen de la protection des données et à l'avis 4/2014 émis par le Groupe de l'article 29. La Cour ne tient pas non plus compte de la résolution 68/167 adoptée par l'Assemblée générale des Nations unies le 18 décembre 2013, des observations finales concernant le quatrième rapport périodique des États-Unis d'Amérique adoptées par le Comité des droits de l'homme (HCR) le 26 mars 2014 et de la déclaration conjointe adoptée le 21 juin 2013 par le Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression et le Rapporteur spécial de la Commission interaméricaine des droits de l'homme sur la liberté d'expression[38]. Plus incroyable encore, la majorité n'examine même pas les documents internationaux disponibles faisant autorité sur le régime britannique d'interception en masse, tels que les observations finales concernant le septième rapport périodique du Royaume-Uni, adoptées le 17 août 2015 par le HCR[39], et le mémorandum du Commissaire aux droits de l'homme du Conseil de l'Europe sur les mécanismes de renseignement et de contrôle au Royaume-Uni, publié en mai 2016[40].

9. Tous ces documents, de même que les arrêts récemment rendus par la Cour dans les affaires *Szábo et Vissy*[41] et *Mustafa Sezgin Tanrıkulu c. Turquie*[42] et la jurisprudence pertinente de la Cour de justice de l'Union européenne (CJUE[43]) contredisent la thèse selon laquelle la surveillance vise majoritairement des personnes qui se trouvent hors de la

[38] Pour une analyse détaillée de ces documents, voir mon opinion séparée jointe à l'arrêt *Szábo et Vissy c. Hongrie*, précité.
[39] ONU, documents officiels, CCPR/C/GBR/CO/7.
[40] CommDH (2016)20.
[41] *Szábo et Vissy*, précité, § 66: « toute personne se trouvant sur le territoire hongrois est susceptible de faire l'objet d'une surveillance secrète ».
[42] *Mustafa Sezgin Tanrıkulu*, précité, § 7.
[43] Paragraphes 209-241 du présent arrêt. Je renvoie ici aux affaires *Digital Rights Ireland Ltd* (où la CJUE a jugé que la directive 2006/24/CE sur la conservation de données « comport[ait] (…) une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne »), *Maximilian Schrems* (où la CJUE a critiqué une réglementation qui permettait aux autorités publiques d'accéder « de manière généralisée au contenu de communications électroniques »), *Privacy International* (où était en cause une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée – qui touchait « l'ensemble des personnes faisant usage de services de communications électroniques » – des données relatives au trafic et des données de localisation aux services de renseignement) et *La Quadrature du Net et autres* (où la CJUE a censuré des dispositions législatives imposant aux fournisseurs de service de conserver de manière « généralisée et indifférenciée » les données relatives au trafic et les données de localisation). Les deux premières affaires portaient sur le traitement de données à caractère personnel à des fins de répression de la criminalité, les deux dernières sur l'appréciation de la surveillance secrète menée par des services de renseignement.

compétence territoriale de l'État. Toutes ces sources dignes de foi confirment au contraire que la surveillance de masse vise principalement des personnes relevant de la compétence territoriale de l'État[44]. Le Gouvernement lui-même a admis que le nombre de demandes d'interception de données de communication fondées sur l'article 8 § 4 de la RIPA et visant des personnes dont on sait qu'elles se trouvent dans les îles Britanniques – demandes qui s'analysent donc en des mesures de surveillance intérieure – s'élève à plusieurs milliers par semaine[45].

10. Le deuxième argument avancé par la majorité pour s'écarter de la jurisprudence antérieure consiste à dire que les États membres du Conseil de l'Europe qui mettent en œuvre un régime d'interception en masse « le font apparemment[46] » à des fins étrangères aux enquêtes pénales. La Cour paraît tenir le raisonnement suivant : dès lors que les interceptions ciblées sont employées – « pour la plupart d'entre elles[47] » – à des fins de détection et d'investigation des infractions dans le cadre de l'interception en masse, mais que l'interception en masse peut aussi servir à collecter des informations dans le cadre du renseignement extérieur, où il peut ne pas y avoir de cibles spécifiques ou d'infractions identifiables, l'interception en masse n'est pas et ne doit pas être gouvernée par les mêmes règles que la surveillance ciblée[48]. Mais là encore, cet argument n'est pas étayé par la Cour, qui préfère se fonder sur des apparences plutôt que sur des faits.

11. En réalité, l'interception en masse non ciblée est expressément ou implicitement interdite dans vingt-trois États européens[49]. Comme l'APCE[50] et le Commissaire aux droits de l'homme du Conseil de l'Europe[51] l'ont démontré avec force, la surveillance massive indiscriminée des

---

[44] Voir ci-dessous l'exposé complet des raisons pour lesquelles la distinction fondée sur la compétence territoriale entre communications extérieures et communications intérieures est inapte à justifier l'interception en masse des communications intérieures.

[45] Voir les observations du gouvernement défendeur devant la Grande Chambre, 2 mai 2019, p. 39 (« plusieurs milliers au cours d'une semaine pour les seuls individus dont on sait ou dont on pense qu'ils se trouvent dans les îles Britanniques »).

[46] Paragraphe 345 du présent arrêt.

[47] *Ibidem*.

[48] Il convient de relever que les gouvernements français et néerlandais ont avancé, à l'instar de la chambre, qu'il est faux de présumer que les interceptions en masse sont plus intrusives pour la vie privée que les interceptions ciblées (paragraphes 300 et 306 du présent arrêt).

[49] Comme l'indique lui-même le rapport de recherche de la Cour en ce qui concerne l'Albanie, Andorre, l'Autriche, la Belgique, la Bosnie-Herzégovine, la Croatie, la Grèce, l'Irlande, l'Islande, l'Italie, le Liechtenstein, la Macédoine du Nord, la Moldova, Monaco, le Monténégro, la Pologne, le Portugal, la République tchèque, la Roumanie, Saint-Marin, la Serbie, la Turquie et l'Ukraine. Le tableau du paysage européen dressé aux paragraphes 242-246 du présent arrêt ne correspond donc pas à la réalité.

[50] APCE, résolution 2031 (2015).

[51] Mémorandum du Commissaire aux droits de l'homme du Conseil de l'Europe sur les mécanismes de renseignement et de contrôle au Royaume-Uni, CommDH (2016)20, mai 2016, p. 10.

communications s'est révélée inefficace pour la prévention du terrorisme et constitue donc non seulement un danger pour la protection des droits de l'homme, mais aussi un gaspillage de ressources. Dans ces conditions, s'il existe en Europe un consensus sur l'interception en masse non ciblée, il est en faveur de l'interdiction de cette pratique, ce dont la Cour ne tient pas compte. Seuls sept États membres du Conseil de l'Europe ont recours à des interceptions en masse non ciblées[52], principalement à des fins de prévention, de détection et d'investigation des infractions de terrorisme, d'espionnage, de cybercriminalité et, plus vaguement, des « infractions graves[53] », comme le montrent les documents de référence susmentionnés, les arrêts *Szábo et Vissy* et *Mustafa Sezgin Tanrıkulu* ainsi que la jurisprudence pertinente de la CJUE. La collecte d'informations dans le cadre du renseignement extérieur n'est qu'un but parmi d'autres, et la Cour n'a pas la moindre preuve, d'ordre statistique ou autre, des méthodes employées pour parvenir à la réalisation de ce but, qu'elles reposent sur la surveillance de cibles spécifiques ou sur d'autres moyens. À supposer même, pour les besoins de la discussion, que la collecte d'informations dans le cadre du renseignement extérieur s'appuie principalement sur des interceptions en masse non ciblées, il ne faut pas nécessairement en conclure que toutes les interceptions en masse, y compris celles qui visent la détection et l'investigation des infractions, doivent être non ciblées. Si tel était le cas, l'interception en masse deviendrait une échappatoire destinée à contourner les garanties inhérentes au mandat individuel dans des situations où un tel mandat serait parfaitement adapté à la collecte des communications recherchées. Cela étant, rien ne s'oppose à ce que la collecte d'informations dans le cadre du renseignement extérieur repose elle aussi sur des interceptions en masse subordonnées à l'existence d'un soupçon raisonnable de participation de la personne ou des personnes visées à des activités préjudiciables à la sécurité nationale, même s'il ne s'agit pas d'infractions pénales[54].

12. Le troisième – et le plus faible – des arguments de la Cour porte précisément sur la frontière ténue entre l'interception ciblée classique et les nouvelles méthodes d'interception en masse utilisées pour cibler des individus précis. La Cour avance qu'« on ne surveille pas les appareils utilisés par les individus ciblés[55] » dans le cadre d'une interception utilisant

[52] Paragraphe 242 du présent arrêt.

[53] Paragraphe 345 du présent arrêt. Je renvoie à cet égard à la critique de la notion d'« infraction grave » formulée par la CJUE (paragraphe 212 du présent arrêt).

[54] Voir le rapport de la Commission de Venise sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique, 2015, pp. 9, 25 et 26 (« il faut des faits concrets attestant d'une conduite s'analysant en une infraction pénale ou en une menace pour la sécurité et les enquêteurs doivent « avoir un motif probable de suspicion », « nourrir un soupçon raisonnable » ou remplir un autre critère analogue »), ainsi que le mémorandum du Commissaire aux droits de l'homme du Conseil de l'Europe, précité, p. 6.

[55] Paragraphe 346 du présent arrêt.

des sélecteurs forts, et que l'interception en masse n'appelle donc pas les mêmes garanties que l'interception ciblée classique. Cela n'est pas convaincant. La collecte et le traitement automatiques au moyen de sélecteurs forts qui permettent l'acquisition de communications à destination ou en provenance d'une cible ou en rapport avec celle-ci acheminées par des canaux de transmission choisis par les services de renseignement constituent une forme d'ingérence potentiellement beaucoup plus intrusive dans les droits garantis par l'article 8 que la simple surveillance des appareils utilisés par des individus ciblés[56]. Il est donc spécieux de déclarer que « seuls » (§ 346) les paquets de communications des individus ciblés sont interceptés et de donner à entendre que l'interception en masse fondée sur des sélecteurs forts est moins intrusive que la surveillance classique des appareils de tel ou tel individu.

C. Un régime de garanties déficient

13. De ce raisonnement entaché d'erreurs de fait, la Cour tire deux conclusions juridiques quant à « l'approche à adopter dans les affaires relatives à l'interception en masse[57] » : il n'est pas obligatoire que la nature des infractions pouvant donner lieu à un mandat d'interception et les catégories de personnes dont les communications sont susceptibles d'être interceptées soient définies dans le droit interne, et il n'est pas nécessaire que les mandats d'interception en masse soient justifiés par l'existence d'un soupçon raisonnable[58]. Dans la logique de la Cour, dès lors que « les interceptions en masse (...) ont en principe un but préventif », à la différence d'« une enquête portant sur une cible précise et/ou une infraction identifiable[59] », aucune des deux garanties susmentionnées n'est requise en droit interne, même lorsqu'une interception en masse vise un individu précis impliqué dans une infraction pénale identifiable. Ainsi, un mandat d'interception général autorisant l'acquisition de communications de personnes sur lesquelles ne pèse aucun soupçon suffit à déclencher une interception en masse, que ce soit à des fins de détection et d'investigation des infractions ou à d'autres fins.

14. La position de la Cour laisse de nombreuses questions en suspens. Quels sont les motifs propres à justifier une interception en masse ? Par exemple, l'investigation des « infractions graves », sans autre précision, constitue-elle un motif justificatif ? Quel degré de gravité l'infraction objet de l'enquête doit-elle présenter ? Une enquête sur le vol d'un portefeuille et

---

[56] Comme la CJUE l'a indiqué dans l'arrêt *Digital Rights Ireland*, précité, § 55, « [l]a nécessité de disposer de (…) garanties est d'autant plus importante lorsque (…) les données à caractère personnel sont soumises à un traitement automatique ».

[57] Point c) iii) de l'appréciation de la Cour.

[58] Paragraphe 348 du présent arrêt.

[59] *Ibidem*.

d'un téléphone mobile constitue-t-elle un motif justificatif[60] ? Le développement de l'espionnage économique et industriel dans l'intérêt de la prospérité économique et de la sécurité nationale de l'État qui procède à l'interception est-il un motif justificatif[61]? Dans quelles « circonstances » est-il acceptable que les communications d'une personne puissent être interceptées ? Quel degré d'intérêt les communications d'un individu doivent-elles présenter au regard des buts poursuivis par un mandat d'interception en masse pour que leur interception en masse puisse passer pour justifiée ? Cet intérêt réside-t-il dans l'existence d'un « soupçon à l'égard de la personne visée », mentionnée dans l'arrêt *Szábo et Vissy*[62], ou d'un soupçon raisonnable, comme le veut le critère énoncé dans l'arrêt *Roman Zakharov*[63] ? Comment la Cour peut-elle exiger que le droit interne énonce « avec suffisamment de clarté[64] » les motifs pour lesquels une interception en masse peut être autorisée et les circonstances dans lesquelles les communications d'un individu sont susceptibles d'être interceptées alors qu'elle-même ne définit pas de manière suffisamment précise la nature des « motifs » et des « circonstances » auxquels elle se réfère ?

15. Dès lors que l'article 8 s'applique à toutes les étapes de l'interception en masse, y compris à la rétention initiale des communications et des données de communication associées[65], c'est à juste titre que la Cour impose la mise en place de « garanties de bout en bout[66] ». Mais le problème est qu'elle ne définit pas précisément la nature juridique de ces « garanties de bout en bout ». D'un côté, elle les présente comme des exigences impératives (« devraient être appréciées[67] », « devraient être soumises[68] », « devrait (...) être autorisée[69] », « devrait être informé[70] », « devraient être tenus de justifier[71] », « devrait être consignée scrupuleusement[72] », « devrait également être soumis[73] », « il est impératif que le recours[74] ») en les qualifiant de « garanties fondamentales[75] », et

[60] Cet exemple est tiré de la jurisprudence de la CJUE (paragraphe 220 du présent arrêt).
[61] Cet exemple reflète les vigoureuses critiques formulées par le Parlement européen dans sa résolution du 12 mars 2014 sur le programme de surveillance de la NSA (États-Unis), par la Commission de Venise dans son rapport précité, p. 21, et par le Commissaire aux droits de l'homme du Conseil de l'Europe dans son mémorandum précité, p. 8.
[62] *Szábo et Vissy*, précité, § 71.
[63] *Roman Zakharov*, précité, §§ 260, 262 et 263.
[64] Paragraphe 348 du présent arrêt.
[65] Paragraphe 330 du présent arrêt.
[66] Paragraphe 350 du présent arrêt.
[67] *Ibidem*.
[68] *Ibidem*.
[69] Paragraphe 351 du présent arrêt.
[70] Paragraphe 352 du présent arrêt.
[71] Paragraphe 355 du présent arrêt.
[72] *Ibidem*.
[73] Paragraphe 356 du présent arrêt.
[74] Paragraphe 359 du présent arrêt.

même de « garanties minimales[76] ». Mais de l'autre, elle les édulcore en précisant qu'elle doit « apprécier globalement le fonctionnement[77] » du régime d'interception, ce qui ouvre la voie au sacrifice de certaines d'entre elles[78]. En définitive, il apparaît qu'aucune des garanties individuelles n'est impérative et que les commandements ainsi énoncés par la Cour ne constituent pas réellement des éléments non négociables dans les ordres juridiques internes. Dans certaines parties de l'Europe, des services secrets zélés seront fortement tentés de profiter du laxisme extrême dont la Cour fait preuve dans la formulation de normes juridiques, et ce seront des innocents qui en paieront tôt ou tard le prix.

D. Conclusion préliminaire

16. La Cour exige qu'une autorité indépendante[79] de l'exécutif intervienne dès le début de l'opération d'interception pour évaluer le but poursuivi par celle-ci, la sélection des canaux de transmission[80] et les catégories de sélecteurs[81] au regard des principes de nécessité et de proportionnalité. Le choix des sélecteurs forts se rapportant à des individus identifiables est particulièrement problématique, car la sélection et « l'utilisation de chaque sélecteur fort[82] » ne sont pas subordonnées à une autorisation préalable indépendante. Pour ces opérations, la Cour se borne à exiger une autorisation interne et la garantie que les demandes de sélecteurs forts soient justifiées et que la procédure interne soit consignée « scrupuleusement[83] ».

17. En outre, l'exécution des mandats d'interception – c'est-à-dire leurs renouvellements, l'utilisation et la conservation des éléments interceptés, la transmission de ces éléments à des tiers et leur suppression – devrait être soumise à la supervision d'une autorité indépendante de l'exécutif, et des archives détaillées devraient être tenues à chaque étape du processus pour que cette supervision s'en trouve facilitée[84].

---

[75] Paragraphe 350 du présent arrêt.
[76] Paragraphe 348 du présent arrêt.
[77] Paragraphe 360 du présent arrêt.
[78] Voir, par exemple, le paragraphe 370, *in fine*, du présent arrêt.
[79] Malgré le manque d'uniformité de la terminologie employée par la Cour, qui utilise en certaines occasions la notion d'autorité indépendante, et en d'autres occasions la notion d'organe indépendant, il ne semble pas que ces deux notions soient substantiellement différentes.
[80] Paragraphe 352 du présent arrêt.
[81] Paragraphe 354 du présent arrêt.
[82] Paragraphe 355 du présent arrêt.
[83] *Ibidem*. Comme l'indique le rapport de la Commission de Venise (précité, p. 33), « les contrôles internes sont insuffisants ». Force est donc de constater que le paragraphe 199 du présent arrêt dénature la position de la Commission de Venise.
[84] Paragraphe 356 du présent arrêt.

18. Finalement, l'ensemble du processus devrait faire l'objet d'un contrôle *a posteriori* dans le cadre d'une procédure équitable et contradictoire, par une autorité indépendante de l'exécutif ayant le pouvoir de rendre des décisions contraignantes, notamment pour ce qui est d'ordonner la cessation d'une interception irrégulière et la destruction des données interceptées obtenues ou conservées de manière illégale, ainsi que des données obsolètes, équivoques ou disproportionnées[85].

III. ÉLABORATION D'UN RÉGIME D'INTERCEPTION EN MASSE *PRO PERSONA*

A. L'interception en masse de communications

19. J'estime que le régime décrit ci-dessus ne présente pas de garanties suffisantes en ce qui concerne les droits protégés par les articles 8 et 10. À mon avis, on ne saurait se passer aujourd'hui des garanties fondamentales que constituent l'autorisation, la supervision et le contrôle *a posteriori* par un juge dans le domaine de l'interception en masse[86]. Sur le plan des principes, la supervision judiciaire de bout en bout des interceptions en masse se justifie par le caractère extrêmement intrusif de cette pratique. Je ne vois pas pourquoi un État régi par la prééminence du droit ne devrait pas faire confiance à ses magistrats en fonction, et en dernier ressort à ses juges les plus chevronnés et expérimentés, pour trancher les questions qui se posent dans ce domaine. À moins que la Cour n'estime que des organes quasi-judiciaires sont plus indépendants que des tribunaux ordinaires...Je considère pour ma part que l'indépendance des organes quasi-judiciaires ne va pas de soi. Par ailleurs, dès lors que les tribunaux ordinaires sont habilités à autoriser, à superviser et à contrôler les interceptions de communications réalisées pour les besoins de procédures pénales très complexes, comme les enquêtes sur la criminalité organisée et le terrorisme, je ne vois pas pourquoi ils seraient incompétents pour exercer les mêmes fonctions en ce qui concerne le fonctionnement d'un processus d'interception en masse. L'indépendance et la compétence des tribunaux ordinaires ne devraient donc pas être remises en cause aux fins de la mise en place, dans un régime d'interception en masse, d'un ensemble de garanties conformes à la Convention. Un État qui pense que ses juges en activité sont

---

[85] Paragraphe 359 du présent arrêt.

[86] Voir le rapport de la Commission de Venise, précité, p. 38 (« [l]es États européens préfèrent généralement un système d'autorisation juridictionnelle préalable »). Force est donc de constater que le paragraphe 197 du présent arrêt dénature le message adressé par la Commission de Venise. Le Commissaire aux droits de l'homme du Conseil de l'Europe a également préconisé l'adoption du système de l'autorisation judiciaire préalable (voir son mémorandum précité, § 28).

inaptes à exercer ces fonctions a un rapport très problématique à la notion de prééminence du droit.

20. L'intervention de la justice n'est certes pas une panacée[87]. Il est évident que la supervision judiciaire de l'ensemble du processus sera vaine si les catégories d'infractions et d'activités et de sujets d'interception à surveiller ne sont pas définies dans le droit interne avec le degré de clarté et de précision qui s'impose. En conséquence, le contrôle judiciaire doit s'étendre au choix concret des canaux de transmission et des sélecteurs forts, c'est-à-dire aux canaux de transmission et aux sélecteurs spécifiquement ciblés, et non à des « types » ou à des « catégories » de canaux de transmission et de sélecteurs, sans quoi l'autorité interceptrice aurait carte blanche pour collecter tout ce qu'elle veut.

21. Dans un système de double verrouillage, où le juge examine des mandats déjà émis par des responsables politiques ou des fonctionnaires, les pouvoirs qui lui sont reconnus dans le cadre de son contrôle ne doivent pas se limiter à la possibilité d'annuler les décisions administratives prises par ces responsables politiques ou fonctionnaires si elles lui semblent déraisonnables. En effet, il n'y aurait pas de véritable autorisation judiciaire en pareil cas, car les critères de nécessité et de proportionnalité posés par la Convention sont plus exigeants que le simple critère du caractère raisonnable.

22. Comme je l'ai indiqué dans l'arrêt *Szábo et Vissy*, la Convention n'autorise pas les recherches « aléatoires » ou « exploratoires » de données, que ce soit sous la forme d'une surveillance non ciblée fondée sur des sélecteurs non spécifiques ou sous la forme d'une surveillance ciblée fondée sur des sélecteurs forts se rapportant à des communications concernant le sujet visé par l'interception[88]. Elle ne permet pas davantage l'élargissement du champ d'une interception par l'utilisation de termes de recherche plus vagues. Je rappelle la raison fondamentale qui m'a conduit à cette conclusion. L'admission des interceptions en masse non ciblées représente un changement majeur de notre conception de la prévention et de l'investigation des infractions ainsi que de la collecte de renseignements en Europe, qui consistait initialement à cibler des suspects identifiables et qui consiste désormais à traiter tout un chacun comme un suspect potentiel dont les données doivent être conservées, analysées et soumises à un profilage[89].

---

[87] Le fait que l'autorisation judiciaire puisse ne pas constituer à elle seule une garantie suffisante contre les abus ne saurait faire conclure qu'elle n'est pas une garantie nécessaire. S'il est vrai que l'IPA a mis en place un mécanisme d'autorisation judiciaire préalable, il ne convient pas ici de débattre *ex professo* de la norme de contrôle juridictionnel instaurée par ce texte, car la loi de 2016 échappe à l'objet du litige dont la Cour est saisie.

[88] Voir l'ensemble des références internationales citées dans mon opinion séparée jointe à l'arrêt *Szábo et Vissy*, précité.

[89] C'est la raison pour laquelle je considère que la collecte massive de données de personnes innocentes admise par la Cour dans le présent arrêt va à l'encontre des principes posés dans les arrêts *S et Marper c. Royaume-Uni* n[os] 30562/04 et 30566/04, § 135,

S'il est vrai que l'impact d'un tel changement sur les personnes innocentes peut éventuellement être atténué par une cohorte d'arbitres et de régulateurs plus ou moins souples et par une pléthore de lois et de codes de conduite plus ou moins appropriés, il n'en demeure pas moins qu'une société reposant sur de telles fondations ressemble davantage à un État policier qu'à une société démocratique, à l'opposé de ce que les pères fondateurs souhaitaient pour l'Europe lorsqu'ils ont signé la Convention en 1950.

23. Il en résulte que toute cible de surveillance doit toujours être identifiée ou identifiable en amont sur le fondement d'un soupçon raisonnable. Pour être parfaitement clair, je précise que l'interception en masse n'est acceptable que si elle est fondée sur des sélecteurs forts concernant les communications en provenance ou à destination du sujet visé par l'interception et s'il existe un soupçon raisonnable de participation de celui-ci à des infractions graves ou à des activités préjudiciables à la sécurité nationale mais non nécessairement criminelles définies par la loi[90].

24. La garantie judiciaire doit s'étendre à l'autorisation de la surveillance des communications et des données de communication associées, notamment des données couvertes par le secret professionnel ou par la confidentialité, à la seule exception des cas d'urgence, lorsque le juge compétent n'est pas immédiatement disponible, auquel cas l'autorisation pourra être délivrée par un procureur sous réserve qu'elle soit ultérieurement entérinée par le juge compétent.

25. Le droit interne doit prévoir un régime spécial de protection des communications couvertes par le secret professionnel des parlementaires, des médecins, des avocats et des journalistes[91]. La collecte de communications en masse systématique visant les communications de

---

4 décembre 2008; *Shimovolos c. Russie*, n° 30194/09, §§ 68 et 69, 21 juin 2011; *M.K. c. France*, n° 19522/09, § 37, 18 avril 2013; et surtout *Mustafa Sezgin Tanrıkulu c. Turquie*, précité, §§ 57-59.

[90] Comme le veut la norme universelle reproduite dans la Compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans la lutte antiterroriste, établie par l'ONU le 17 mai 2010 (A/HRC/14/46) : « Pratique n° 21. Le droit interne définit: le type de mesures de recherche de renseignements à la disposition des services secrets; les objectifs de la recherche de renseignements autorisés; les catégories de personnes et d'activités pouvant être visées par la recherche du renseignement; le niveau de suspicion requis pour justifier le recours à des mesures de recherche du renseignement; la durée maximum d'application desdites mesures; et la procédure d'autorisation, de contrôle et d'analyse du recours à ces mesures ».

[91] Outre *Sanoma Uitgevers B.V. c. Pays-Bas* [GC], n° 38224/03, §§ 90-92, 14 septembre 2010, voir Agence des droits fondamentaux de l'Union européenne (FRA), « *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, volume II*: Field perspectives and legal updates* », 2017, p. 12 (« [l]es États membres devraient établir des procédures juridiques spécifiques pour protéger le secret professionnel de groupes tels que les membres du parlement, les magistrats, les avocats et les professionnels des médias. La mise en œuvre de ces procédures devrait être contrôlée par un organe indépendant » [traduction du greffe]).

personnes sur lesquelles ne pèse aucun soupçon étant susceptible de faire échec à la protection des informations couvertes par le secret professionnel ou la confidentialité, cette protection ne peut être effectivement garantie que si leur interception est soumise à l'autorisation d'un juge et subordonnée à la production de preuves faisant naître un soupçon raisonnable de participation des professionnels concernés à une infraction grave ou à une activité préjudiciable à la sécurité nationale[92]. En outre, toute communication de ces catégories de professionnels couverte par le secret professionnel doit être immédiatement détruite si elle a été interceptée par erreur. Le droit interne doit également prévoir l'interdiction absolue de toute interception des communications couvertes par le secret religieux.

26. Le contrôle judiciaire ne doit pas s'arrêter à la phase initiale du processus d'interception. Si le fonctionnement réel du système d'interception était caché au juge, l'intervention initiale de celui-ci pourrait être aisément mise à mal et privée de tout effet utile, ce qui en ferait une garantie virtuelle et illusoire. Le juge doit au contraire encadrer l'ensemble du processus en examinant de manière régulière et vigilante la nécessité et la proportionnalité du mandat d'interception, au regard des données qui ont été interceptées. Faute de recevoir en permanence des remontées d'information de la part de l'autorité interceptrice, le juge qui a délivré l'autorisation ne peut pas savoir comment celle-ci est utilisée en pratique. Si l'utilisation qui en est faite n'est pas conforme au mandat, le juge doit pouvoir y mettre fin immédiatement et ordonner la destruction des données obtenues illégalement. Tel doit être également le cas lorsque la poursuite de l'opération n'est pas nécessaire, par exemple parce que les données obtenues ne présentent aucun intérêt au regard des buts poursuivis par le mandat d'interception. Seul un juge compétent pour prendre pareilles décisions contraignantes est en mesure de garantir de manière effective la légalité des données conservées. En résumé, le juge doit être habilité à contrôler régulièrement le fonctionnement du système, y compris l'intégralité des enregistrements des interceptions et des documents classifiés y afférents[93], pour pouvoir prévenir toute atteinte non nécessaire et disproportionnée aux droits garantis par les articles 8 et 10.

---

[92] Rapport de la Commission de Venise, précité, p. 31.

[93] Comme le veut la règle universelle et européenne reproduite, d'une part, dans la compilation précitée des Nations unies (« Pratique n° 25. Une institution indépendante existe pour contrôler l'utilisation faite des données personnelles par les services de renseignement. Cette institution a accès à tous les fichiers détenus par lesdits services et elle est habilitée à ordonner la divulgation d'informations aux personnes concernées, ainsi que la destruction des fichiers ou des renseignements personnels qu'ils contiennent ») et, d'autre part, dans le rapport précité de la FRA, p. 11 (« [l]es États membres devraient également autoriser les organes de contrôle à lancer leurs propres enquêtes de leur propre initiative et à accéder de manière permanente, totale et directe aux informations et aux documents nécessaires à l'accomplissement de leur mandat » [traduction du greffe]).

27. Enfin, le contrôle *a posteriori* de l'utilisation d'un mandat d'interception devrait aussi pouvoir être déclenché par la notification de celui-ci à la personne ciblée. Lorsque rien ne s'oppose à ce que la personne dont les communications ont été interceptées en soit avisée, cette notification lui permettrait de contester les motifs de l'interception dans le cadre d'une procédure équitable et contradictoire[94]. Dans ces conditions, il est pour le moins extrêmement hypothétique d'affirmer qu'un système qui n'est pas lié à une notification « pourrait même offrir de meilleures garanties de procédure régulière qu'un système fondé sur la notification[95] ». Le sujet de l'interception est le mieux placé pour défendre ses propres intérêts.

28. Lorsque, pour une raison ou pour une autre, notamment dans l'intérêt de la sécurité nationale, il est impossible de notifier à la personne concernée que ses communications ont été interceptées, celle-ci n'a en pratique aucun moyen de prendre connaissance de la mesure de surveillance dont elle a fait l'objet. En pareil cas, il est impératif que le juge soit habilité à examiner, d'office ou à la demande d'un tiers (par exemple, un procureur), la manière dont le mandat a été exécuté pour déterminer si les données obtenues ont été collectées légalement et si elles doivent être conservées ou détruites, étant entendu que la personne ciblée doit être représentée par un avocat commis d'office pour la protection des données.

29. Enfin, et ce n'est pas le moins important, les ressources humaines et financières et les moyens techniques affectés à la supervision doivent être à la mesure des opérations à superviser, faute de quoi le système ne sera qu'une simple façade dissimulant les pratiques administratives discrétionnaires des autorités interceptrices.

B. L'échange de données interceptées avec des services de renseignement étrangers

30. La Cour abaisse le niveau de protection applicable au transfert à des services de renseignement étrangers de données obtenues au moyen d'une interception en masse. Premièrement parce qu'elle n'oblige pas l'État qui transfère ces données à s'assurer que l'État destinataire dispose de garanties d'un niveau équivalent aux siennes. En outre, elle n'exige pas que l'État auteur du transfert demande à l'État destinataire, avant chaque transfert, de lui donner l'assurance qu'il mettra en place des garanties propres à prévenir

[94] *Szábo et Vissy*, précité, § 86. Dans la logique de l'arrêt *Szábo et Vissy*, il s'agit là d'une exigence distincte qui se superpose aux critères *Weber et Saravia*. Pour une explication sur les avantages d'une procédure de notification pour « limiter l'utilisation excessive », voir le rapport de la Commission de Venise, précité, p. 41, et les rapports du Commissaire aux droits de l'homme du Conseil de l'Europe sur l'Allemagne (p. 17) et le Royaume-Uni (2016, précité, p. 5).

[95] Paragraphe 358 du présent arrêt.

les abus et les ingérences disproportionnées lors du traitement des données transférées[96]. En d'autres termes, la Cour n'exclut pas que des données puissent être transférées en masse à un service de renseignement étranger selon un processus continu dans un objectif unique. Compte tenu du caractère fortement discrétionnaire de ce régime, on ne sait pas au juste en quoi consiste le « contrôle indépendant » exigé par la Cour[97]. Quel est l'intérêt d'un contrôle indépendant s'il n'est pas nécessaire d'évaluer les garanties mises en place par l'État destinataire (et notamment de s'assurer que celui-ci s'engage à « garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties[98] ») avant chaque transfert ? Le contrôle indépendant est-il limité aux situations dans lesquelles « il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles[99] » ? Pour qui cela doit-il être clair, pour le service de renseignement qui procède au transfert ou pour le juge ? Existe-t-il une différence entre un contrôle indépendant et une autorisation indépendante ? L'imprécision des termes employés par la Cour paraît servir son intention d'édulcorer les garanties spécifiques qui s'attachent au transfert lui-même.

31. J'estime que cet abaissement du niveau de la protection conventionnelle en ce qui concerne l'échange de données de masse ne repose sur aucune justification, et je constate que la Cour n'en fournit aucune. Selon les normes communes au Conseil de l'Europe et à l'Union européenne, le partage de données à caractère personnel doit être circonscrit aux pays tiers qui assurent un niveau de protection substantiellement équivalent à ceux que le Conseil de l'Europe et l'Union européenne garantissent respectivement[100]. Le contrôle judiciaire doit être aussi approfondi dans ce domaine que dans les autres, à plus forte raison lorsqu'un État membre du Conseil de l'Europe transmet des données à un État non membre, pour la raison évidente que l'utilisation que ce dernier

---

[96] Paragraphe 362 du présent arrêt.
[97] *Ibidem*.
[98] *Ibidem*.
[99] *Ibidem*.
[100] La majorité ignore le fait que l'article 2 du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181) dispose que les parties doivent assurer un niveau de protection adéquat aux transferts de données à caractère personnel vers des États tiers, et qui n'admet des dérogations que lorsque des intérêts légitimes prévalent. Le rapport explicatif de ce Protocole ajoute que les exceptions doivent être interprétées de manière restrictive, « afin que l'exception ne devienne pas la règle » (§ 31). Il importe de relever que ce Protocole a été ratifié par quarante-quatre États, dont huit ne sont pas membres du Conseil de l'Europe. Le Royaume-Uni ne l'a pas ratifié. Parallèlement à cette norme du Conseil de l'Europe, l'Union européenne n'autorise le transfert de données à caractère personnel que vers des pays tiers qui assurent un niveau de protection substantiellement équivalent à celui garanti dans l'Union européenne (§ 234 du présent arrêt).

fera des données transférées échappera à la compétence de la Cour. Ce contrôle judiciaire ne doit pas être limité par la « règle du tiers service », qui interdit aux services de renseignement de divulguer à un tiers des données reçues d'un service de renseignement étranger sans le consentement de la source[101].

C. L'interception en masse de données de communication associées

32. Enfin, la Cour reconnaît que l'interception en masse de données de communication associées revêt potentiellement un caractère extrêmement intrusif[102], sans pour autant leur accorder le même niveau de protection[103]. D'un côté, elle exige que « les garanties énoncées ci-dessus [au paragraphe 361 du présent arrêt] soient en place », mais de l'autre elle admet que les États membres peuvent choisir les garanties à incorporer dans leur droit interne puisqu'« il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications[104] ». Le message véhiculé par la Cour est si confus qu'il ne donne aux États aucune indication utile qui leur permettrait de déterminer lesquelles des « garanties énoncées ci-dessus » sont obligatoires, si tant est que certaines le soient, en ce qui concerne l'interception en masse de données de communication associées. L'indécision dont la Cour fait preuve n'atténue nullement le risque – qu'elle évoque elle-même – que ces données permettent de brosser un portrait détaillé de toutes les relations sociales des personnes concernées.

D. Conclusion préliminaire

33. Je ne souscris pas à la conclusion selon laquelle « si les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet [la protection de la sécurité

---

[101] Voir le rapport de la Commission de Venise, précité, 2015, p. 40 (« [l]e principe de la maîtrise de l'information par son auteur ne saurait s'appliquer à un organe de contrôle »), ainsi que le rapport de la FRA, « *Surveillance by intelligence services* », précité, p. 12 (« (n]onobstant la règle du tiers service, les États membres devraient envisager d'accorder aux organes de contrôle un accès total aux données échangées dans le cadre de la coopération internationale. Cela étendrait leurs pouvoirs de contrôle à toutes les données disponibles traitées par les services de renseignement » [traduction du greffe]).

[102] Paragraphe 342 du présent arrêt.

[103] En fin de compte, la Cour s'est laissée influencer par la menace du gouvernement défendeur, qui a déclaré que « [s]i les États membres qui mettent en œuvre un régime d'interception en masse étaient tenus d'appliquer les mêmes protections aux RCD [données de communications associées] qu'au contenu, on aboutirait sans doute à une dilution de la protection du contenu » (observations du gouvernement défendeur devant la Grande Chambre, 2 mai 2019, p. 39).

[104] Voir le paragraphe 364 du présent arrêt combiné avec le paragraphe 361.

nationale ou de tout autre intérêt national essentiel contre des menaces extérieures graves], la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte[105] ». Si les États jouissent d'une ample latitude, le contrôle dont ils feront l'objet, aussi strict soit-il, ne suffira pas à assurer une protection contre les abus. La marge d'appréciation applicable à l'élaboration d'un système d'interception et à son fonctionnement doit être identique, et elle doit être étroite compte tenu du caractère extrêmement intrusif des pouvoirs de surveillance qu'un tel système confère aux États, du risque élevé d'abus qui lui est inhérent et, il faut le rappeler, du consensus européen en faveur de la prohibition de l'interception en masse non ciblée.

34. En résumé, la législation interne doit user de termes assez clairs pour indiquer de manière suffisante aux individus et aux personnes morales[106] les conditions impératives et les procédures à différents niveaux que la puissance publique doit respecter pour pouvoir recourir à l'interception en masse. Ces conditions et procédures sont notamment les suivantes[107] :

a) Les motifs propres à justifier la délivrance d'un mandat d'interception doivent être définis. Ils englobent notamment la détection d'activités menaçant la sécurité nationale ainsi que la prévention, la détection et l'investigation d'infractions graves, sous réserve que les infractions susceptibles de déclencher une interception correspondent à des infractions graves précisément énumérées ou, plus généralement, à des infractions passibles d'une peine d'emprisonnement non inférieure à quatre ans[108] ;

b) Les sujets d'interception doivent être définis. Il s'agit des personnes ou institutions dont les communications sont susceptibles d'être interceptées selon les modalités suivantes :

> i) les recherches aléatoires ou exploratoires visant à découvrir des « inconnues inconnues », notamment les formes de surveillance non ciblée fondée sur des sélecteurs non spécifiques, doivent être catégoriquement interdites ;
>
> ii) l'utilisation de sélecteurs forts visant des communications en rapport avec les sujets d'interceptions ciblés doit être catégoriquement interdite ;
>
> iii) l'utilisation de sélecteurs forts visant les communications en provenance ou à destination des sujets d'interception ciblés peut être autorisée lorsqu'il existe des

[105] Paragraphe 347 du présent arrêt.

[106] Dans l'affaire *Liberty et autres*, précitée, les requérantes étaient toutes des ONG qui alléguaient que leur droit à la protection de leur correspondance avait été violé. Ce droit se trouve également en cause dans la présente affaire.

[107] Pour établir cette liste, je me suis fondé non seulement sur les références citées au paragraphe 8 de la présente opinion, mais aussi sur la compilation des Nations unies, précitée, 2010, sur le rapport de la Commission de Venise, précité, 2015, et sur le rapport de la FRA, précité, 2017.

[108] L'article 2 b) de la Convention des Nations unies contre la criminalité transnationale organisée dispose que l'expression « infraction grave » désigne un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde. L'exposé des motifs de la recommandation Rec(2005)10 du Comité des Ministres suit cette indication.

soupçons raisonnables de participation de ces derniers aux infractions ou activités susmentionnées.

c) Les formes de communications électroniques susceptibles d'être interceptées, notamment les communications par téléphone, télex ou fax, les adresses de courrier électronique, les recherches sur Google, la navigation sur Internet, les médias sociaux et le stockage de données dans le « Cloud » doivent être répertoriées ;

d) Le principe de nécessité doit être respecté, ce qui implique :

i) que l'ingérence dans les droits des sujets d'interception corresponde aux buts poursuivis et qu'elle n'aille pas au-delà de ce qui est nécessaire à leur réalisation ;

ii) que l'interception ne se justifie qu'en dernier recours, lorsqu'il n'existe aucun autre moyen d'obtenir des preuves ou des informations, soit parce que le recours à des méthodes moins intrusives s'est révélé infructueux soit, par exception, parce qu'il paraît peu probable que d'autres méthodes moins intrusives aboutissent ;

iii) que l'interception soit conçue de manière à éviter, autant que possible, de viser des personnes ou des institutions n'ayant aucune part dans les infractions ou activités susmentionnées ;

iv) que l'interception prenne immédiatement fin lorsqu'elle ne sert plus les buts poursuivis.

e) Le principe de proportionnalité doit être respecté, ce qui implique :

i) qu'un juste équilibre soit ménagé entre les droits des sujets d'interception et les buts poursuivis, en vertu du principe selon lequel plus les infractions ou activités susmentionnées et leurs conséquences passées ou futures sont graves, plus l'interception pourra être intrusive et étendue ;

ii) que l'interception doit en tout état de cause garantir le respect de la substance (ou du noyau dur) des droits des sujets d'interception, notamment le droit des personnes physiques à la vie privée intime. L'interception doit prendre fin dès qu'il apparaît qu'elle empiète sur un domaine essentiel de la vie privée.

f) La durée des mandats d'interception doit être limitée. Elle pourra être prolongée une ou plusieurs fois après évaluation des résultats de l'opération, mais une durée maximale doit en tout état de cause être fixée pour l'ensemble de l'opération ;

g) Une supervision judiciaire de bout en bout doit être instaurée. Elle doit s'étendre :

i) à l'autorisation des interceptions, notamment au choix concret des canaux de transmission ciblés et des sélecteurs forts à utiliser ;

ii) au contrôle régulier, à des intervalles suffisamment courts, de l'exécution des mandats d'interception, de leur prorogation et de la transmission des données obtenues à des tiers, et ;

iii) au contrôle *a posteriori* du processus d'interception et des données interceptées.

h) En cas d'urgence, un procureur doit pouvoir délivrer un mandat spécial d'interception, sous réserve que celui-ci soit entériné par un juge à bref délai ;

i) La procédure à suivre pour l'examen, l'utilisation, la conservation et la destruction des données obtenues doit être fixée et s'accompagner d'une description détaillée de l'étendue du contrôle exercé par le juge tant au stade de l'exécution de l'interception qu'à l'issue de celle-ci ainsi que d'un récapitulatif des principales étapes de l'effacement des données dans la mesure où cela est nécessaire au contrôle exercé par le juge ;

j) Les conditions à remplir et les précautions à prendre en ce qui concerne l'échange de données interceptées avec des services de renseignement étrangers doivent être définies de la manière suivante :

> i) l'externalisation des opérations de surveillance en contournement des dispositions du droit interne doit être absolument interdite ;
>
> ii) la divulgation à un tiers de données obtenues par un service de renseignement auprès d'un service de renseignement étranger doit être absolument interdite si la source n'y a pas consenti, sans que cette interdiction puisse limiter l'accès du juge de l'État destinataire aux données transférées ;
>
> iii) l'échange de données avec des services de renseignement étrangers qui n'assurent pas un niveau de protection substantiellement équivalent à celui garanti par la Convention doit être absolument interdit ;
>
> iv) le transfert en masse de données à un service de renseignement étranger et la réception en masse de données transmises par un service de renseignement étranger selon un processus continu poursuivant un but unique doivent être absolument interdits ;
>
> v) chaque transfert ou réception de données doit faire l'objet d'une autorisation judiciaire préalable obéissant à des règles et à des principes exactement identiques à ceux qui s'appliquent aux interceptions en masse intérieures, notamment les principes de nécessité et de proportionnalité ;
>
> vi) les règles susmentionnées s'appliquent indifféremment aux données sollicitées et aux données non sollicitées, aux données « brutes » (non évaluées) et aux données évaluées.

k) L'interception doit être notifiée aux sujets d'interception lorsqu'elle a pris fin, sauf lorsque cette notification risquerait de nuire aux intérêts de la sécurité nationale, auquel cas le juge compétent doit être habilité à examiner, d'office ou à la demande d'un tiers (par exemple, un procureur), l'ensemble du processus d'interception pour déterminer si les données obtenues ont été collectées légalement et si elles doivent être conservées ou détruites, étant entendu que la personne ciblée doit être représentée par un avocat commis d'office pour la protection des données ;

l) Des garanties spéciales protégeant le secret des communications professionnelles des personnes dont les communications sont couvertes par le secret professionnel, notamment les parlementaires, les avocats, les journalistes et les prêtres doivent être mises en place ;

m) Le principe selon lequel une condamnation pénale ne peut être fondée uniquement ou principalement sur des preuves recueillies au moyen d'une interception en masse doit être garanti ;

n) Les principes susmentionnés doivent s'appliquer tant aux opérations de surveillance menées par les Parties contractantes sur leurs territoires respectifs qu'aux opérations de surveillance extraterritoriales, quels que soient le but des opérations en question, l'état des données concernées (stockées ou en transit) ou leurs détenteurs (les sujets d'interception ou les fournisseurs de services) ;

o) Le devoir de l'État de respecter et de faire respecter les droits des individus doit être assorti de l'obligation de protéger ces droits contre les abus commis par des acteurs non-étatiques tels que des sociétés.

IV. CRITIQUE DU RÉGIME BRITANNIQUE D'INTERCEPTION EN MASSE EN CAUSE DANS LA PRÉSENTE AFFAIRE

A. L'interception en masse de communications mise en place par la RIPA de 2000

35. Compte tenu de ce qui précède, le régime britannique d'interception en masse, tel qu'applicable au 7 novembre 2017 – c'est-à-dire avant l'entrée en vigueur complète de la loi de 2016 sur les pouvoirs d'enquête (*Investigatory Powers Act* 2016[109]) – m'inspire une objection de principe qui va bien au-delà des minces reproches que la Grande Chambre lui adresse.

36. La définition donnée par l'article 81 § 2 b) de la RIPA à l'un des buts assignés à l'interception en masse, à savoir la détection et l'investigation des infractions graves, était tout à fait incompatible avec la notion d'infraction grave qui prévaut en droit international puisqu'elle englobait les infractions passibles d'une peine d'emprisonnement inférieure à quatre ans. En outre, le but consistant à sauvegarder la prospérité économique du Royaume-Uni dans la mesure où celle-ci relevait aussi de l'intérêt de la sécurité nationale n'était pas suffisamment précis, si bien qu'il autorisait le recours à l'interception en masse à des fins d'espionnage économique et industriel et de « guerre commerciale[110] », par exemple.

37. La formulation très générale des mandats ministériels délivrés en vertu de l'article 8 § 4 de la RIPA a été critiquée, à juste titre, par la commission parlementaire sur le renseignement et la sécurité [111]

[109] Paragraphe 270 du présent arrêt. Il s'ensuit qu'à l'instar de la Grande Chambre, je n'ai pas tenu compte des modifications introduites par l'IPA et par le nouveau code de conduite en matière d'interception de communications adopté en 2018, dont la Cour n'était pas saisie.

[110] Les parties ont eu une discussion intéressante sur ce point au cours de l'audience qui s'est tenue devant la Grande Chambre le 10 juillet 2019. La position de la Cour sur la précision du but relatif à la sécurité nationale est variable (comparer avec *Iordachi et autres c. Moldova*, n° 25198/02, § 46, 10 février 2009, et *Kennedy c. Royaume-Uni*, précité, § 159).

[111] Paragraphe 146 du présent arrêt.

(*Intelligence and Security Commission of Parliament* – « la commission parlementaire »).

38. La distinction opérée entre les communications intérieures et les communications extérieures par l'article 20 de la RIPA était fondamentalement défectueuse et elle ne restreignait pas suffisamment les catégories de personnes dont les communications étaient susceptibles d'être interceptées. Comme l'a déclaré la commission parlementaire, cette distinction était déroutante et manquait de transparence[112].

39. Pour justifier cette distinction, le Gouvernement a indiqué que « [l]orsqu'ils acquièrent des renseignements sur des activités à l'étranger, les services de renseignement n'ont pas la même capacité à identifier les cibles ou détecter les menaces qu'au Royaume-Uni[113] ». L'IPT a retenu cet argument, déclarant qu'« il était plus difficile d'enquêter sur des projets terroristes ou criminels ourdis à l'étranger[114] ». Cette justification doit être replacée dans le contexte de la note de divulgation présentée par le Gouvernement en 2014, dans laquelle celui-ci reconnaissait que des demandes de données de masse étaient adressées à un service de renseignement étranger « hors du cadre d'un accord d'entraide internationale[115]». En élaborant le système d'interception en masse litigieux, les autorités entendaient donc échapper aux procédures coûteuses en temps et nécessitant des ressources considérables ainsi qu'aux obligations plus « rigoureuses » découlant du cadre de l'entraide judiciaire mis en place par le droit international, autrement dit contourner les garanties instaurées par le système international des traités d'entraide existant et tirer parti de son manque de régulation des nouvelles technologies de surveillance transnationale.

40. Qui plus est, compte tenu de l'accroissement du nombre de communications considérées comme étant extérieures[116] et de l'augmentation exponentielle de l'interception en masse des communications toujours plus nombreuses échangées par des personnes qui se trouvent dans les îles Britanniques[117], il n'est plus techniquement

---

[112] Paragraphe 145 du présent arrêt.

[113] Voir les observations du gouvernement défendeur devant la Grande Chambre, 2 mai 2019, p. 8.

[114] Paragraphe 51 du présent arrêt, repris par la Cour au paragraphe 375.

[115] Paragraphes 36 et 116 du présent arrêt, qui renvoient au paragraphe 12.2 du code de conduite.

[116] Paragraphe 47 du présent arrêt.

[117] Comme l'a indiqué le gouvernement défendeur, « [m]ais le fait que les communications électroniques puissent emprunter n'importe quelle voie pour atteindre leur destination implique qu'une proportion des communications acheminées sur un canal de transmission entre le Royaume-Uni et un autre État constituera des communications internes, c'est-à-dire des communications entre des personnes qui se trouvent dans les îles Britanniques » (voir les observations du gouvernement défendeur devant la Grande Chambre, 2 mai 2019, p. 19).

possible de maintenir la distinction opérée entre les communications extérieures et les communications intérieures, qui se trouve donc privée de sens. La distinction fondée sur la compétence territoriale entre communications extérieures et intérieures est en soi contradictoire avec la réalité actuelle des flux de communications sur Internet, où un message Facebook échangé au sein d'un groupe d'amis à Londres sera considéré comme « extérieur » au Royaume-Uni parce qu'il aura été acheminé via la Californie[118]. Comme la Law Society l'a rappelé à la Cour, le régime découlant de l'article 8 § 4 permettait l'interception des communications confidentielles échangées entre les avocats et leurs clients, même si les premiers comme les seconds se trouvaient au Royaume-Uni[119]. En pratique, la conception large des communications extérieures adoptée par le Gouvernement englobait également le stockage de données dans le « Cloud », les recherches sur Google ainsi que les activités de navigation sur Internet et d'utilisation des médias sociaux[120]. La distinction entre les communications extérieures et les communications intérieures pourrait même s'avérer impossible pour bon nombre de catégories de communications, car les données de communication associées ne révèlent pas toujours la localisation du destinataire. Dans certains cas, l'analyse factuelle du caractère extérieur ou intérieur d'une communication ne peut être effectuée qu'avec du recul[121]. L'interconnexion croissante des modes de vie et de communication à travers les frontières qui caractérise notre époque ne milite certainement pas en faveur d'une différence de traitement entre les communications extérieures et les communications intérieures, bien au contraire. Il va sans dire que ce constat ne doit pas être considéré comme une invitation à abaisser le niveau de protection des communications intérieures, mais à accroître celui des communications extérieures.

41. À cet égard, il ne va pas de soi qu'une communication échangée entre une personne se trouvant à Strasbourg et une personne se trouvant à Londres soit moins digne de protection au regard de la Convention qu'une communication échangée entre deux personnes se trouvant à Londres. La différence de traitement opérée entre ces personnes ne paraît donc reposer sur aucune raison objective de nature à la justifier, mais plutôt sur l'hypothèse que les menaces proviennent plus souvent de l'étranger, et que les étrangers sont moins dignes de confiance que les nationaux parce qu'ils représentent une menace plus grave pour la sécurité nationale et la sûreté publique que les nationaux, ce qui justifierait la surveillance des

[118] Paragraphe 75 du présent arrêt.
[119] Paragraphe 321 du présent arrêt. Voir aussi le jugement rendu par l'IPT dans l'affaire *Belhadj & Others v the Security Service & Others*, IPT/13/132-9/H.
[120] Paragraphe 75 du présent arrêt. Cette pratique paraît contrevenir au paragraphe 6.5 du code de conduite.
[121] Le gouvernement défendeur lui-même l'a admis (voir ses observations devant la Grande Chambre, 2 mai 2019, p. 34).

communications envoyées ou reçues en dehors des îles Britanniques[122]. Cette idée transparaît également dans la manière dont les étrangers sont traités devant la justice lorsqu'ils tentent de faire valoir leur droit à la vie privée. L'IPT ne reçoit pas les plaintes de requérants qui se trouvent hors du territoire national[123]. Cette *Weltanschauung* inamicale envers les étrangers ne peut être plus éloignée de l'esprit et de la lettre de la Convention[124]. C'est l'individu que la Convention place en son centre, et non le citoyen de tel ou tel État, ce qui implique que la protection accordée par les droits conventionnels, qui sont des droits de l'individu, devrait entrer en jeu à chaque fois que l'action d'une Partie contractante est susceptible d'entraîner un besoin de protection, où que ce soit, vis-à-vis de qui que ce soit et de quelque façon que ce soit. En outre, les droits conventionnels devraient transparaître dans la participation des États membres du Conseil de l'Europe à la communauté internationale, dans la mesure où « l'ordre juridique du Conseil de l'Europe ne peut plus être assimilé à un accord international d'égoïsmes juxtaposés. La souveraineté n'est plus une donnée absolue, comme à l'époque westphalienne, elle est partie intégrante d'une communauté au service des droits de l'homme[125] ».

42. En définitive, force est de constater que la distinction opérée par la RIPA était inadaptée à l'époque de l'avènement de l'ère d'Internet, et qu'elle n'avait qu'un but politique qui consistait à justifier le système mis en place aux yeux de la population britannique en lui donnant l'illusion que

---

[122] On ne peut se contenter d'affirmer, comme l'a fait la chambre au paragraphe 517 de son arrêt, que dès lors que la législation britannique « empêche que les éléments interceptés ne soient sélectionnés pour examen selon un facteur « lié à un individu dont on sait qu'il se trouve actuellement dans les îles Britanniques », si l'interception constituait une différence de traitement celle-ci reposerait, non pas directement sur la nationalité ou l'origine nationale, mais plutôt sur la situation géographique », car il est évident que la grande majorité des personnes dont on sait qu'elles se trouvent actuellement dans les îles Britanniques sont des citoyens britanniques, et qu'à l'inverse la majorité des personnes qui ne s'y trouvent pas sont des étrangers. Le traitement plus favorable réservé aux nationaux a également été souligné dans le rapport de la FRA, « *Surveillance by intelligence services* », précité, p. 45 (« [l]es garanties légales applicables aux activités de surveillance intérieure menées par les services de renseignement sont plus solides que celles qui s'appliquent à la surveillance extérieure » [traduction du greffe]).

[123] Voir IPT, *Human Rights Watch & Ors v SoS for the Foreign & Commonwealth Office & Ors*, 16 mai 2016: « Un requérant qui allègue que des activités relevant de l'article 68 § 5 de la RIPA sont menées par un service de renseignement ou pour le compte de celui-ci doit démontrer que cette allégation est fondée, afin de prouver qu'il est potentiellement exposé au risque d'être visé par ces activités. Il doit également démontrer, à l'appui de son allégation, qu'il se trouvait au Royaume-Uni à l'époque pertinente ».

[124] Le rapport de la Commission de Venise, précité, p. 20, a formulé la même critique pour des « raisons fondamentales », de même que le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, qui s'est appuyé sur le PIDCP (paragraphe 313 du présent arrêt).

[125] Voir le paragraphe 22 de mon opinion séparée jointe à l'arrêt *Mursic c. Croatie* [GC], n° 7334/13, 20 octobre 2016.

les personnes relevant de la compétence territoriale du Royaume-Uni échapperaient au Big Brother gouvernemental, ce qui était faux. Le ministre compétent était habilité à ordonner quand il le jugeait nécessaire l'examen d'éléments sélectionnés selon un facteur lié à un individu qui se trouvait dans les îles Britanniques[126] et à modifier un certificat pour autoriser la sélection des communications de cet individu[127]. En outre, la capture accidentelle de communications intérieures non visées par un mandat délivré par le ministre était autorisée à chaque fois qu'elle était nécessaire à la collecte de communications extérieures visées par un mandat[128], situation dont le Gouvernement lui-même a admis qu'elle était « en pratique inévitable[129] ». Cela dit, il convient de relever que l'interception en masse de données de communication associées n'était même pas limitée par la restriction relative aux communications extérieures.

43. Même si l'interception en masse était conçue comme un instrument de collecte de renseignements extérieurs[130] plutôt que comme un outil de prévention, de détection et d'investigation des infractions[131], cette circonstance ne justifiait pas le manque d'encadrement et l'étendue des pouvoirs conférés aux autorités interceptrices. En tout état de cause, en raison du développement des communications numériques, la garantie limitant les interceptions aux communications extérieures n'est plus une restriction réelle[132], si elle l'a jamais été. Et j'estime qu'elle ne l'a jamais été, pour les raisons exposées ci-dessous.

44. Les mandats relevant de l'article 8 § 4 de la RIPA étaient délivrés par un ministre non indépendant[133] et se présentaient comme des chèques en blanc qui ne mentionnaient pas le nom du sujet de l'interception et qui ne le décrivaient pas, qui ne limitaient pas expressément le nombre de communications susceptibles d'être interceptées et qui ne comportaient aucune précision quant aux canaux de transmission visés et aux sélecteurs utilisés. À l'exception des dispositions anodines contenues dans les paragraphes 4.28 à 4.31 du code de conduite[134], aucune règle particulière ne

[126] Article 16 § 3 de la RIPA.
[127] Paragraphe 6.2 du code de conduite.
[128] Article 5 § 6 a) de la RIPA et paragraphe 6.6 du code de conduite.
[129] Observations du gouvernement défendeur devant la Grande Chambre, 2 mai 2019, p. 35.
[130] Le paragraphe 6.2 du code de conduite énonçait que « les interceptions réalisées en vertu de l'article 8 § 4 sont un moyen d'obtenir des renseignements ».
[131] L'article 81 de la RIPA donnait une définition de la prévention et de la détection des infractions, mais il ne définissait pas l'investigation.
[132] Le rapport de la Commission de Venise, précité, p. 13, fait le même constat.
[133] Dans le rapport de la commission parlementaire publié en 2015, avant les changements induits par l'introduction de l'IPA en 2016, le parlement britannique a admis le manque d'indépendance du ministre.
[134] Dispositions applicables aux éléments relevant de l'article 8 § 4 de la RIPA sélectionnés pour examen et constituant des informations confidentielles (paragraphe 4.32 du code de conduite). Le gouvernement défendeur reconnaît désormais que « les demandes portant sur des données de communication et visant à identifier des sources journalistiques doivent être

régissait les situations où étaient formulées des demandes visant les communications d'un journaliste, d'un médecin ou d'un prêtre ou qui étaient susceptibles de conduire à une intrusion collatérale dans ces communications. Le choix des canaux de transmission et l'application de sélecteurs – même de sélecteurs forts – aux communications extérieures dépendaient en dernier ressort de l'autorité interceptrice[135]. En clair, la communauté du renseignement contrôlait entièrement la procédure d'autorisation et tenait le ministre à distance de toutes les informations essentielles, si bien que celui-ci était dans l'incapacité d'évaluer correctement tant la proportionnalité que la nécessité des interceptions et que son rôle se réduisait à apporter une caution politique au fonctionnement du système[136].

45. En outre, le code de conduite édicté par le ministre n'était pas contraignant puisqu'il était permis d'y déroger pour de justes motifs. Pis encore, le travail quotidien des analystes était soumis à des « procédures non publiques » inaccessible à la population, même sous une forme résumée ou expurgée[137]. Cette latitude administrative accordée à l'autorité interceptrice méconnaissait l'objectif du principe de légalité, selon lequel les règles qui régissent l'interception en masse doivent avoir une base en droit interne, et être accessibles et prévisibles quant à leurs effets.

46. L'insuffisance de la réglementation du régime en cause était aggravée par le statut du Commissaire à l'interception des communications (« le commissaire »), qui n'était pas une autorité indépendante et n'exerçait pas un contrôle effectif sur la mise en œuvre des mandats d'interception[138]. Le rapport de la commission parlementaire publié en 2015 indique que « bien que les deux commissaires soient d'anciens juges, ils exercent leurs fonctions de commissaire hors du cadre judiciaire officiel », et il conclut que « certaines des fonctions qu'ils exercent actuellement n'ont pas de base légale. Cette situation est insatisfaisante et inappropriée[139] ». Mais là n'est pas le pire, car le statut juridique du commissaire présentait des défauts

---

soumises à une autorisation judiciaire » (réponse du Royaume-Uni au mémorandum du Commissaire aux droits de l'homme du Conseil de l'Europe sur les mécanismes de renseignement et de contrôle au Royaume-Uni, p. 24 [traduction du greffe]).

[135] Paragraphes 146-147 du présent arrêt.

[136] Dans son rapport de 2015, la commission parlementaire est parvenue à la même conclusion (paragraphe 147 du présent arrêt). Dans ces conditions, il n'est guère surprenant que 3007 mandats d'interception aient été émis en 2016 et que cinq demandes aient été refusées par un ministre (paragraphe 170 du présent arrêt). Ces chiffres sont éloquents : le rôle du ministre se bornait à apposer son cachet sur les demandes qui lui étaient présentées.

[137] Paragraphe 33 du présent arrêt.

[138] Voir le paragraphe 347 de l'arrêt de la chambre et le paragraphe 26 de l'opinion séparée de la juge Koskelo, à laquelle s'est ralliée la juge Turković, qui relève que le système de garanties du régime britannique était encore plus déficient que celui du régime allemand en vigueur à l'époque des affaires *Klass et autres* et *Weber et Saravia*.

[139] La majorité néglige malheureusement de tenir compte de ce passage du rapport de la commission parlementaire publié en 2015, mentionné au paragraphe 142 du présent arrêt.

encore plus graves. La loi conférait au Premier ministre le pouvoir de nommer le commissaire, lequel devait lui rendre compte de l'accomplissement de sa mission et dépendait du ministre compétent du point de vue de sa dotation en personnel[140]. Qui plus est, le commissaire exerçait ses fonctions à temps partiel et pouvait être révoqué à tout moment par le Premier ministre[141]. Pareil statut était à l'évidence incompatible avec l'indépendance que supposait un contrôle effectif du fonctionnement du régime découlant de l'article 8 § 4 de la RIPA. En résumé, le commissaire n'était pas « institutionnellement, opérationnellement et financièrement indépendant des institutions qu'il était chargé de superviser », comme l'exigent les principes de Tshwane[142].

47. À supposer même, pour les besoins de la discussion, que le commissaire exerçait un contrôle indépendant au Royaume-Uni, force est de constater que celui-ci n'était pas effectif, pour la simple raison que lorsque le commissaire découvrait une erreur grave, ses pouvoirs se résumaient à adresser au Premier ministre un rapport pour lui signaler cette erreur et, le cas échéant, à décider dans quelle mesure celle-ci pouvait être rendue publique[143]. Il n'était pas habilité, par exemple, à signaler le problème à l'IPT ou à informer la victime d'une interception abusive. D'ailleurs, il n'a même pas remarqué qu'Amnesty International et le South African Legal Resources Centre avaient fait l'objet d'une surveillance illégale !

48. La loi ne fixait aucune limite précise à la durée maximale des interceptions et de la conservation des données, et la pratique ne comblait pas cette lacune[144]. Les mandats relevant de l'article 8 § 4 de la RIPA pouvaient être prorogés *ad aeternam*[145]. En outre, les durées de conservation différaient en fonction des agences interceptrices[146], dont les hauts responsables pouvaient déroger de leur propre chef à la durée maximale « normale » fixée par le paragraphe 7.9 du code de conduite (à savoir deux ans). Cela en dit long sur les véritables orchestrateurs du système d'interception en masse britannique[147].

---

[140] Article 57 de la RIPA de 2000.

[141] La critique formulée par les requérantes lors de l'audience tenue devant la Grande Chambre le 10 juillet 2019 est légitime : un juge unique retraité travaillant à temps partiel avec l'assistance d'un secrétariat restreint, et dont la tâche consiste à procéder à des analyses par sondage, « ne peut espérer exercer un contrôle significatif ».

[142] Sur ces principes et leur rôle au sein du Conseil de l'Europe, voir mon opinion séparée jointe à l'arrêt *Szábo et Vissy*, précité.

[143] Comme l'a reconnu le gouvernement défendeur lors de l'audience tenue devant la Grande Chambre le 10 juillet 2019.

[144] Comme l'a indiqué le gouvernement défendeur au paragraphe 403 du présent arrêt. Il semblerait que même les procédures internes n'étaient pas respectées (paragraphe 59 du présent arrêt).

[145] Paragraphes 6.22 à 6.24 du code de conduite.

[146] Paragraphe 176 du présent arrêt.

[147] Il est proprement stupéfiant que la majorité ait jugé seulement « souhaitable », au paragraphe 405 du présent arrêt, que la pratique indiquée par le gouvernement défendeur au

49. La loi ne prévoyait aucune obligation d'informer la personne concernée à l'issue du processus d'interception[148]. Or en l'absence de pareille information, le droit d'accès à un tribunal est largement illusoire. Tel était le cas au Royaume-Uni[149]. L'IPT ne pouvait intervenir que s'il était saisi d'une plainte par une personne pensant avoir fait l'objet d'une surveillance secrète, ce qui en faisait une garantie purement théorique pour tous les sujets d'interception auxquels rien ne laissait penser que leurs communications avaient été interceptées[150]. Le caractère insuffisant du contrôle exercé par l'IPT était aggravé par le fait qu'il n'était pas un « tribunal » au sens de l'article 4 de la loi de 1998 sur les droits de l'homme – et qu'il n'avait donc pas compétence pour prononcer une déclaration d'incompatibilité lorsqu'il estimait que la législation primaire était incompatible avec la Convention, que ses décisions étaient insusceptibles de recours et, étrangement, que l'adoption de son règlement de procédure relevait de la compétence du ministre, ce qui signifiait concrètement que l'organe contrôlé avait le pouvoir de fixer les règles gouvernant l'organe contrôleur[151].

B. L'échange de données interceptées avec des services de renseignement étrangers

50. Il n'existait pas de cadre législatif exprès analogue à la RIPA habilitant le gouvernement britannique à utiliser les données interceptées par des pays étrangers. Ce n'est qu'en janvier 2016 que le chapitre 12 du code de conduite a instauré un cadre régissant ces échanges[152]. Le

---

cours de la procédure suivie devant la Grande Chambre soit consacrée par la loi.

[148] L'IPA impose désormais au commissaire de rechercher s'il y a eu une erreur grave et s'il serait dans l'intérêt général d'informer la personne concernée, mais la Cour n'est pas saisie de cette disposition dans la présente affaire. L'introduction de cette mesure dans l'IPA équivaut à une reconnaissance des lacunes du système antérieur, mais le moment n'est pas venu de déterminer si cette solution suffira.

[149] Et la politique du gouvernement défendeur consistant à ne rien confirmer ni démentir aggravait cette situation, car elle « empêchait à jamais les personnes de savoir si elles ont fait l'objet d'une surveillance » et « mettait les décisions de surveillance à l'abri d'un contrôle effectif », comme l'a observé le Commissaire aux droits de l'homme du Conseil de l'Europe dans son mémorandum précité.

[150] Force est donc de constater que la conclusion de la majorité selon laquelle l'IPT « offrait un recours juridictionnel solide à toutes les personnes qui pensaient que leurs communications avaient été interceptées par les services de renseignement » (§ 415) passe à côté du vice flagrant qui entachait ce système, à savoir son caractère purement virtuel pour les personnes qui n'avaient aucune raison de soupçonner qu'elles avaient fait l'objet d'une surveillance secrète.

[151] Article 69 § 1 de la RIPA.

[152] Le gouvernement défendeur a déclaré que « même avant la publication du chapitre 12 du code de conduite, il était « accessible » grâce à la note de divulgation », c'est-à-dire la note de divulgation d'octobre 2014 (voir les observations du Gouvernement devant la Grande chambre, 2 mai 2019, p. 45). Force est donc de constater que le Gouvernement

paragraphe 12.5 de ce code et la note de bas de page qui l'accompagnait autorisaient les autorités à demander à des services de renseignement étrangers des communications interceptées et les données de communication associées « à destination ou en provenance de sélecteurs spécifiques, ou en rapport avec de tels sélecteurs[153] ». La NSA a cessé en avril 2017 d'intercepter des communications « en rapport » avec des cibles, car pareilles interceptions ne pouvaient effectuées légalement en raison de leur caractère beaucoup trop intrusif[154]. Or l'étonnante propension de la Cour à accepter la politique du gouvernement défendeur consistant à « tout recueillir[155] » dépasse même les objectifs stratégiques de la NSA puisqu'elle la conduit à admettre non seulement les demandes d'interception « en rapport » avec une cible, mais aussi les demandes d'éléments non liés à des sélecteurs spécifiques[156].

51. Selon la Cour, la transmission d'informations obtenues au moyen d'une interception en masse à des partenaires de renseignement étrangers devrait être soumise à un « contrôle indépendant[157]», mais pas la réception d'informations obtenues au moyen d'une interception en masse réalisée par des services de renseignement étrangers[158]. Pourtant, dès lors que les garanties encadrant la surveillance directe exercée par les autorités interceptrices britanniques ont été jugées insuffisantes, elles auraient dû être jugées tout aussi insuffisantes en ce qui concerne la surveillance indirecte exercée par ces autorités grâce aux données interceptées transmises par des tiers, à plus forte raison lorsque les données en question étaient collectées par des tiers non liés par la Convention. C'est dans cette situation, où le risque que des données soient collectées et conservées d'une manière non conforme était le plus élevé et qu'un contrôle indépendant était par conséquent le plus nécessaire, que la Cour renonce à cette garantie sans aucune justification plausible[159]. À cet égard, la supervision exercée par le commissaire et l'IPT, invoquée par le Gouvernement et la majorité de la Grande Chambre, était en pratique aussi inopérante en ce qui concerne le

---

lui-même admet que la loi n'était pas accessible avant cette époque.

[153] Paragraphe 116 du présent arrêt.

[154] Paragraphe 263 du présent arrêt.

[155] Lors de l'audience tenue devant la Grande Chambre le 10 juillet 2019, le gouvernement défendeur s'est exprimé ainsi : « si la question qui pose problème consiste à savoir si nous avons beaucoup de données, même après le processus de filtrage, la réponse est « oui », et c'est une fort bonne chose à notre avis ».

[156] Paragraphes 502 et 503 du présent arrêt.

[157] Paragraphe 362 du présent arrêt.

[158] Paragraphe 513 du présent arrêt.

[159] La Cour ne tient malheureusement pas compte de la position du Comité des droits de l'homme qui, dans ses observations finales de 2015 sur le Royaume-Uni (ONU, documents officiels, CCPR/C/GBR/CO/7, 17 août 2015, par. 24), a exprimé des préoccupations au sujet de « l'insuffisance des garanties entourant l'obtention de communications privées auprès de services de sécurité étrangers et le partage de données de communication personnelles avec ces services ».

contrôle de l'échange d'éléments interceptés par des tiers qu'en ce qui concerne le contrôle de la surveillance intérieure, puisque l'IPT ne pouvait intervenir que s'il était saisi d'une plainte et que les pouvoirs du commissaire se résumaient à adresser un rapport un Premier ministre pour lui signaler des erreurs graves.

52. Les conséquences absurdes du raisonnement de la majorité apparaissent de manière encore plus flagrante dans l'exemple suivant : si un londonien adresse à un autre londonien un message Twitter acheminé par un serveur situé aux États-Unis, la Cour admettra que l'interception de ce message et des données de communication associées par le service britannique du renseignement électronique (*Government Communications Headquarters* – « le GCHQ ») au moment où il quitte le Royaume-Uni via un câble en direction des États-Unis doit être soumise à la garantie d'une autorisation indépendante. En revanche, si la NSA intercepte ce même message à l'autre extrémité du même câble et en transmet une copie ou les données de communication associées au GCHQ, la garantie d'une autorisation indépendante ne s'appliquera pas. Cette différence dans la protection juridique accordée aux mêmes données, fondée uniquement sur la circonstance fortuite que l'auteur de l'interception initiale se trouve à tel ou tel endroit, est totalement arbitraire. Faute d'avoir encadré l'utilisation des données interceptées obtenues auprès de pays tiers par un régime de garanties légales aussi protecteur que celui applicable aux données interceptées sur le territoire national[160], la législation du Royaume-Uni ne fournissait pas une protection suffisante contre l'arbitraire et les abus.

53. En outre, il ressort du paragraphe 12.6 du code de conduite que les articles 15 et 16 de la RIPA ne s'appliquaient pas à toutes les communications obtenues auprès d'un service de renseignement étranger qui pouvaient être le produit d'une interception, mais seulement à celles dont l'interception avait été sollicitée et qui se « présent[ai]ent comme le produit d'une interception », si bien que l'applicabilité des garanties prévues par le droit interne de l'État destinataire (en l'occurrence, le Royaume-Uni) était subordonnée à une décision des services de renseignement étrangers.

54. Cette description du régime du partage de données interceptées en masse avec d'autres parties serait incomplète si j'omettais de mentionner une autre particularité remarquable. Il convient de préciser que le paragraphe 7.3 du code de conduite autorisait la divulgation d'éléments interceptés à d'autres parties à la seule convenance du service concerné, critère étonnamment sommaire. Le principe du « besoin d'en connaître[161] » est l'exact opposé des principes de nécessité et de proportionnalité : le principe selon lequel seuls les éléments interceptés dont une personne a besoin de prendre connaissance peuvent lui être communiqués est

[160] C'est exactement ce que préconise la Commission de Venise (paragraphe 201 du présent arrêt).

[161] Paragraphe 7.3 du code de conduite (paragraphes 96 et 390 du présent arrêt).

l'antithèse de ces principes. L'usage de ce pouvoir de divulgation n'était subordonné à aucun critère légal objectif, mais seulement guidé – et éventuellement dévoyé – par le but poursuivi. Il était donc admis que des considérations purement opportunistes devaient prévaloir sur une appréciation de la nécessité et de la proportionnalité de l'atteinte supplémentaire aux droits des sujets d'interception que constitue la divulgation des éléments interceptés à d'autres parties. Pour le dire simplement, les communications des individus étaient considérées comme des biens appartenant à l'État, des produits que celui-ci pouvait partager avec des tiers comme bon lui semblait pour « savoir s'il y avait une aiguille dans la botte de foin[162] ».

C. L'interception en masse de données de communications associées

55. Enfin, l'article 16 § 2 de la RIPA ne s'appliquait pas à l'interception en masse de données de communications associées, si bien que n'importe quel analyste pouvait utiliser un sélecteur fort lié à un individu dont on savait qu'il se trouvait dans les îles Britanniques sans avoir besoin d'un certificat d'autorisation préalablement délivré par le ministre compétent, et pis encore, les données ainsi interceptées pouvaient être conservées « quelques mois » si et aussi longtemps qu'elles étaient nécessaires à la découverte d'« inconnues inconnues[163] ». Concrètement, l'interception et le traitement des données de communications associées n'étaient limités que par les capacités de stockage des services d'interception. À vrai dire, la RIPA ne constituait pas réellement un instrument de collecte de renseignements extérieurs, car les avancées technologiques en avaient fait un outil de surveillance intérieure, raison pour laquelle le Gouvernement soutient désormais que la garantie applicable aux îles Britanniques contenue dans l'article 16 de la RIPA n'était pas « nécessaire » pour assurer la conformité du système à la Convention[164].

56. L'argument du Gouvernement qui consiste à exciper d'une infaisabilité technique[165] ne me convainc pas davantage. Il est tout à fait possible, pour un juge, d'apprécier en temps utile et au cas par cas la nécessité et la proportionnalité d'une demande d'autorisation de ciblage des données de communication associées de tel ou tel individu sans risque

[162] Voir la plaidoirie du gouvernement défendeur à l'audience tenue devant la Grande Chambre le 10 juillet 2019.
[163] Paragraphes 422-423 du présent arrêt.
[164] Voir la plaidoirie du gouvernement défendeur à l'audience tenue devant la Grande Chambre le 10 juillet 2019. De cette manière, l'autorité interceptrice pouvait se procurer, au moyen d'un mandat d'interception en masse, des données de contenu qu'elle aurait dû obtenir au moyen d'un mandat individuel et ciblé relevant de l'article 8 de la RIPA, ce qui lui permettait de contourner l'arrêt rendu par la Cour dans l'affaire *Kennedy c. Royaume-Uni*, précité.
[165] Paragraphe 420 du présent arrêt.

majeur d'en compromettre l'utilisation[166]. Si – comme l'admet la Cour[167] – la mise en place d'un tel dispositif d'autorisation est possible lorsque les cibles sont des journalistes ou des membres d'autres professions dont les données de communications associées sont couvertes par le secret professionnel, pourquoi ne serait-elle pas possible lorsque les cibles sont les données de communication associées du commun des mortels ? La mise en place d'un dispositif d'autorisation fonctionnant à grande échelle est tout à fait réalisable. Le fait est que des atteintes de grande ampleur à la vie privée appellent un système de garanties de grande ampleur.

57. Eu égard à l'étendue de l'intrusion dans la vie privée résultant de ces pratiques, tant dans les îles Britanniques qu'en dehors de celles-ci, la tolérance de la Cour à leur endroit est incompréhensible, d'autant qu'elle considère elle-même que l'article 16 § 2 de la RIPA était « la principale garantie légale encadrant le processus de sélection pour examen d'éléments interceptés[168] ».

D. Conclusion préliminaire

58. En résumé, le fait que les activités de surveillance examinées dans les affaires *Weber et Saravia* (2006) et *Liberty et autres* (2008) étaient nettement plus restreintes que celles qui ont actuellement cours n'aurait pas dû conduire la Cour à être moins exigeante en ce qui concerne le niveau de protection de la vie privée que l'on est en droit d'attendre aujourd'hui. L'augmentation exponentielle de la surveillance au cours de la dernière décennie et le tollé général qu'elle suscite appellent un renforcement du contrôle des activités des services de renseignement dans le but de préserver la démocratie et la prééminence du droit, et non l'inverse. L'aggravation du risque d'abus des pouvoirs de l'État exige un renforcement des garanties conventionnelles et de celles qui leur correspondent en droit interne, non un affaiblissement de ces garanties[169]. Autrement dit, les exigences de la Cour

---

[166] Je me fonde ici sur ma propre expérience de juge pénal ayant siégé dans des affaires criminelles très complexes, où il arrivait souvent que la police demande l'interception d'un très grand nombre de données de communication associées.

[167] Paragraphe 450 du présent arrêt.

[168] Rapprocher et comparer les §§ 420 et 421. On notera que la Cour qualifie cette disposition de « principale garantie légale » au § 420, avant de la reléguer au rang d'« importante garantie » au § 421. Si l'imprécision du langage employé au § 421 est déroutante, la faiblesse de l'argumentation qui y est développée est encore plus préoccupante. La démarche de la Cour consistant à ne pas accorder le même poids aux « préoccupations » exprimées aux §§ 381 et 382 pour ce qui est de l'interception en masse de données de communication associées passe par la manipulation pure et simple du langage. Mais la cerise sur le gâteau est bien sûr le recours à « l'appréciation globale », qui permet à la Cour de parvenir au résultat qui lui convient, quel qu'il soit (voir mon analyse du critère de l'« équité globale » dans les opinions séparées que j'ai jointes aux arrêts *Muhammad et Muhammad c. Roumanie* [GC], n° 80982/12, 15 octobre 2020, et *Murtazaliyeva c. Russie* [GC], n° 36658/05, 18 décembre 2018).

devraient être plus strictes aujourd'hui qu'en 2006 ou en 2008. Or c'est exactement le contraire qui se dégage du présent arrêt, où la Cour s'incline devant le fait accompli de l'interception en masse généralisée, en se rendant à l'argument dangereux qu'il faut l'autoriser parce qu'elle est utile. Mais l'utilité ne se confond pas avec la nécessité et la proportionnalité dans une société démocratique. Comme l'a dit le juge Brandeis dans l'arrêt *Olmstead v. United States*[170], « de même, peu importe que l'intrusion [une écoute téléphonique] contribue à assurer le respect de la loi. Nous devrions savoir par expérience que la plus grande vigilance s'impose pour défendre la liberté lorsque le gouvernement poursuit des objectifs bien intentionnés ».

V. CONCLUSION

59. Le présent arrêt modifie fondamentalement l'équilibre ménagé en Europe entre le droit au respect de la vie privée et les intérêts de la sécurité publique en ce qu'il cautionne la surveillance non ciblée du contenu des communications électroniques et des données de communication associées, et pis encore, l'échange de données avec des pays tiers qui ne disposent pas d'un niveau de protection comparable à celui des États du Conseil de l'Europe. Ce constat apparaît d'autant plus justifié à la lumière du refus catégorique que la CJUE a opposé à l'accès généralisé au contenu des communications électroniques[171], de sa réticence manifeste envers la conservation générale et indifférenciée des données de trafic et des données de localisation[172], et des limitations qu'elle a imposées au partage de données avec des services de renseignement étrangers n'assurant pas un niveau de protection substantiellement équivalent à celui garanti par la Charte des droits fondamentaux[173]. Sur ces trois points, la Cour de Strasbourg reste en retrait de la Cour de Luxembourg, qui demeure le phare de la protection de la vie privée en Europe.

60. Pour le meilleur ou pour le pire – pour le pire selon moi, l'arrêt de la Cour ouvre la voie à un « Big Brother » électronique en Europe. Si telle est la nouvelle normalité que mes éminents collègues de la majorité souhaitent pour l'Europe, je ne puis m'y rallier, et je le dis le cœur lourd, avec la même désolation que celle qui émane du *Miserere mei, Deus* de Gregorio Allegri.

---

[169] *Szábo et Vissy*, précité, § 70 : « Les garanties exigées en l'état actuel de la jurisprudence de la Convention sur les interceptions doivent être renforcées pour répondre aux problèmes soulevés par ces pratiques de surveillance ». De même, la résolution 2045(2015) de l'APCE souligne la nécessité d'un renforcement du contrôle de la surveillance de masse.

[170] 277 US 438.

[171] Paragraphe 226 du présent arrêt.

[172] Paragraphes 211, 217 et 239-241 du présent arrêt.

[173] Paragraphe 234 du présent arrêt.

OPINION EN PARTIE DISSIDENTE COMMUNE AUX JUGES LEMMENS, VEHABOVIĆ, RANZONI ET BOŠNJAK

(Traduction)

1. Nous souscrivons au présent arrêt, sauf en ce qui concerne l'appréciation, au regard des articles 8 et 10 de la Convention (points 3 et 5 du dispositif de l'arrêt), du grief relatif à la réception, par les autorités de l'État défendeur, d'éléments interceptés demandés à des services de renseignement étrangers.

2. Pour réduire autant que possible le risque d'abus des pouvoirs d'interception prévus par les régimes d'interception en masse, la Grande Chambre a mis en place dans le présent arrêt – ainsi que dans l'arrêt rendu ce jour dans l'affaire *Centrum för Rättvisa c. Suède*, n° 35252/08 – un système de garanties « de bout en bout » effectives dont les trois principaux piliers ou pierres angulaires sont 1) la soumission des opérations d'interception en masse, dès le départ – c'est-à-dire dès la définition de leur objet et de leur étendue, à l'autorisation d'un organe indépendant du pouvoir exécutif ; 2) la soumission de l'emploi de sélecteurs forts liés à des individus identifiables à une autorisation interne préalable ; 3) la supervision des opérations d'interception en masse par une autorité indépendante, conjuguée à un contrôle *a posteriori* effectif exercé par un organe indépendant de l'exécutif (paragraphes 350-359 de l'arrêt).

3. Les régimes qui permettent à des autorités ne pratiquant pas elles-mêmes l'interception de communications transfrontières et des données de communications associées de demander à des services de renseignement étrangers d'intercepter de telles communications ou de leur transmettre des communications déjà interceptées devraient être encadrés par des garanties identiques aux garanties « de bout en bout » applicables aux régimes d'interception en masse. Pourtant, si les garanties relatives à l'examen, à l'utilisation, à la conservation, à la transmission à des tiers, à l'effacement et à la destruction des éléments interceptés sont applicables à l'identique dès la réception des éléments en question (paragraphe 498 de l'arrêt), le premier pilier – l'autorisation indépendante préalable – est totalement passé sous silence dans le raisonnement de la majorité, qui ne nous convainc pas sur ce point. Pourquoi faudrait-il établir une distinction en fonction de la manière dont les autorités ont obtenu les données interceptées, à savoir par une interception directe ou par une interception réalisée à leur demande par une autorité étrangère ? Nous estimons pour notre part que les garanties applicables à l'interception en masse devraient aussi s'appliquer à l'identique dans ce cas de figure, y compris celle qui relève du premier pilier.

4. Nous souscrivons pleinement aux constats opérés par la Cour aux paragraphes 496 et 497 de l'arrêt, où il est notamment énoncé qu'une

ingérence dans les droits garantis par l'article 8 peut se produire dès le stade de la demande initiale d'éléments interceptés adressée aux autorités étrangères et que la protection accordée par la Convention se trouverait vidée de sa substance si les États pouvaient contourner leurs obligations conventionnelles en sollicitant des données interceptées auprès d'États non contractants. La Cour en conclut que les États membres doivent se doter de normes claires et précises offrant des garanties effectives contre l'utilisation de ce pouvoir à des fins de contournement de leur droit interne et/ou de leurs obligations conventionnelles.

5. Notre divergence avec la majorité porte sur la question de savoir en quoi consistent ces « garanties effectives ».

6. En premier lieu, la majorité indique que les demandes de données étaient fondées sur un mandat déjà autorisé ou expressément approuvé par le ministre compétent (paragraphe 505 de l'arrêt). Toutefois, nous estimons que ce ministre n'était pas indépendant de l'exécutif et que le régime régissant la réception de renseignements provenant de services de renseignement étrangers souffrait à cet égard des mêmes lacunes que le régime d'interception en masse (paragraphe 377 de l'arrêt).

7. En second lieu, la majorité semble postuler qu'une législation interne interdisant le contournement de ses dispositions constitue en soi une garantie effective (paragraphe 506 de l'arrêt). Nous ne sommes pas de cet avis. Comme cela a déjà été souligné, notamment dans l'opinion séparée jointe par le juge Ranzoni à l'arrêt *Breyer c. Allemagne* (n° 50001/12, 30 janvier 2020), le droit interne fournit uniquement la base légale qui permet d'apprécier la légalité d'une ingérence ; il ne constitue pas en sus et en soi une garantie effective propre à protéger les individus contre l'application arbitraire de la législation interne par les autorités nationales et contre l'utilisation abusive des pouvoirs conférés par la loi. Cette protection doit aller au-delà des normes juridiques, surtout lorsque ces normes et pouvoirs juridiques sont formulés en des termes généraux.

8. Pour le dire autrement, une disposition légale interdisant le contournement ou d'autres abus ne peut en même temps garantir que pareilles pratiques ne se produiront pas. Pour qu'une garantie soit effective, il faut qu'il existe un mécanisme propre à assurer l'application correcte de la disposition en question. Or il n'existe aucune garantie de ce type en ce qui concerne les demandes d'interception et de transmission de données adressées à des services de renseignement étrangers. Nous estimons que le premier pilier des garanties « de bout en bout » applicables au régime d'interception en masse devrait s'appliquer à l'identique à ces demandes, qui devraient donc être soumises à l'autorisation préalable d'un organe indépendant apte à apprécier leur nécessité et leur proportionnalité au but poursuivi (paragraphes 350 à 351 de l'arrêt) et à veiller à ce que ce pouvoir ne soit pas utilisé pour contourner le droit interne et/ou les obligations conventionnelles des États.

9. C’est pourquoi nous avons voté contre le constat de non-violation de l’article 8 de la Convention en ce qui concerne la réception de renseignements obtenus auprès de services de renseignement étrangers.

10. La majorité ayant conclu à la non-violation de l’article 10 de la Convention à raison du régime d’échange de renseignements pour les mêmes motifs que ceux qui l’ont conduite à conclure à la non-violation de l’article 8 (paragraphe 516 de l’arrêt), nous ne pouvons non plus nous rallier à la conclusion à laquelle elle est parvenue sur le terrain de l’article 10.

ANNEXE

Liste des requérantes

Nº de requête	Requérantes
58170/13	Big Brother Watch
58170/13	English PEN
58170/13	Open Rights Group
58170/13	Dr Constanze Kurz
62322/14	58170/13
62322/14	Alice Ross
24960/15	Amnesty International Limited
24960/15	Bytes For All
24960/15	The National Council for Civil Liberties (« Liberty »)
24960/15	Privacy International
24960/15	The American Civil Liberties Union
24960/15	The Canadian Civil Liberties Association
24960/15	The Egyptian Initiative For Personal Rights
24960/15	The Hungarian Civil Liberties Union
24960/15	The Irish Council For Civil Liberties Limited
24960/15	The Legal Resources Centre