EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRANDE CHAMBRE

AFFAIRE CENTRUM FÖR RÄTTVISA c. SUÈDE

(Requête n° 35252/08)

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 • Carences à raison de l'absence de règle claire concernant la destruction des éléments interceptés qui ne contiennent pas de données à caractère personnel, de l'absence d'obligation de prendre en compte les intérêts liés à la vie privée lorsqu'une décision de partage de renseignements avec des partenaires étrangers est adoptée, du double rôle de l'Inspection du renseignement extérieur et de l'absence de décisions motivées lors du contrôle *a posteriori*, non suffisamment compensées par des garanties

STRASBOURG

25 mai 2021

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

En l’affaire Centrum för rättvisa c. Suède,

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 les 11 juillet, 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 trouve une requête (n° 35252/08) dirigée contre le Royaume de Suède et dont une fondation suédoise, Centrum för rättvisa (« la requérante »), a saisi la Cour le 14 juillet 2008 en vertu de l’article 34 de la Convention de sauvegarde des droits de l’homme et des libertés fondamentales (« la Convention »).

2. La requérante a été représentée par M^es^ F. Bergman et A. Evans, avocats à Stockholm. Le gouvernement suédois (« le Gouvernement ») a été représenté par son agente, M^me^ E. Hammarskjöld, directrice générale des affaires juridiques au ministère des Affaires étrangères.

3. La requérante allègue que la législation et la pratique suédoises en matière de renseignement d’origine électromagnétique portent à ses droits une atteinte constitutive d’une violation de l’article 8 de la Convention. Elle soutient également qu’elle ne dispose d’aucun recours effectif au sens de l’article 13 de la Convention.

4. La requête a été attribuée à la troisième section de la Cour (article 52 § 1 du règlement de la Cour). Le 1^er^ novembre 2011 (recevabilité) et le 14 octobre 2014 (recevabilité et fond), elle a été communiquée au

Gouvernement. Une chambre de cette section, composée de Branko Lubarda, président, de Helena Jäderblom, Helen Keller, Pere Pastor Vilanova, Alena Poláčková, Georgios A. Serghides, Jolien Schukking, juges, ainsi que de Stephen Phillips, greffier de section, a rendu un arrêt le 19 juin 2018. La chambre, à l'unanimité, a déclaré la requête recevable et conclu qu'il n'y avait pas eu violation de l'article 8 de la Convention et qu'il n'y avait pas lieu d'examiner séparément le grief formulé sur le terrain de l'article 13.

5. Le 19 septembre 2018, la requérante a demandé 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 cette demande.

6. La composition de la Grande Chambre a été arrêtée conformément aux articles 26 §§ 4 et 5 de la Convention et 24 du règlement. Le président de la Grande Chambre a décidé que, dans l'intérêt d'une bonne administration de la justice, l'affaire devait être attribuée à la même Grande Chambre que l'affaire *Big Brother Watch et autres c. Royaume-Uni* (nos 58170/13 et 2 autres) (articles 24, 42 § 2 et 71 du règlement).

7. Tant la requérante que le Gouvernement ont déposé des observations écrites sur le fond de l'affaire (article 59 § 1 du règlement).

8. Le président de la Grande Chambre a autorisé les gouvernements estonien, français, néerlandais et norvégien à intervenir dans la procédure écrite (articles 36 § 2 de la Convention et 44 § 3 du règlement).

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

Ont comparu :

– *pour le Gouvernement*

Mmes E. HAMMARSKJÖLD, directrice générale des affaires juridiques au ministère des Affaires étrangères, *agente*,
G. ISAKSSON, directrice adjointe au ministère des Affaires étrangères,
J. SJÖSTRAND, conseillère juridique principale au ministère des Affaires étrangères,

MM. J. GARTON, directeur général adjoint au ministère de la Défense,
M. ANDERSSON, conseiller juridique principal au ministère de la Défense,
H. SELLMAN, directeur adjoint au ministère de la Justice,

Mmes F. KRZYZANSKI, conseillère juridique au ministère des Infrastructures,
M. DRÁB, directrice des affaires juridiques à l'Institut National de la défense radio,

M. C. HELLSTEN, conseiller principal à l'Institut national de la défense radio, *conseillers* ;

– *pour la requérante*

M^es^	F. BERGMAN,	*conseil,*
	A. EVANS,	*conseil,*
M.	A. OTTOSSON,	*conseil,*
M^me^	E. PALM,	*conseillère.*

La Cour a entendu en leurs déclarations M^es^ Evans et Bergman, ainsi que M^me^ Hammarskjöld.

EN FAIT

10. La requérante, Centrum för rättvisa, est une fondation créée en 2002 dont le siège se trouve à Stockholm.

11. Elle représente ses clients dans des procédures concernant les droits et libertés découlant de la Convention et du droit suédois. Elle est également impliquée dans des projets de formation et de recherche et participe au débat public général sur différentes questions concernant les droits et libertés individuels.

12. Elle communique quotidiennement avec des particuliers, des organisations et des entreprises en Suède et à l'étranger par courrier électronique, par téléphone et par télécopie. Elle affirme qu'une large part de ses communications est particulièrement sensible du point de vue du respect de la vie privée. Compte tenu de la nature de son rôle en tant qu'organisation non gouvernementale contrôlant attentivement les activités d'acteurs étatiques, elle estime qu'il y a un risque que ses communications aient été ou soient à l'avenir interceptées et examinées dans le cadre des activités de renseignement d'origine électromagnétique.

13. Elle n'a engagé aucune procédure au niveau interne, et elle plaide à cet égard qu'il n'existe pas en Suède de recours effectif pour ses griefs fondés sur la Convention.

LE CADRE ET LA PRATIQUE JURIDIQUES PERTINENTS

I. LE DROIT ET LA PRATIQUE INTERNES

A. Sur le renseignement d'origine électromagnétique (ROEM) en général

14. Le renseignement d'origine électromagnétique (ROEM) peut être défini comme l'activité consistant à intercepter, traiter, analyser et rapporter des informations transmises par signaux électroniques. Ces signaux peuvent être convertis en texte, en image ou en son. Les renseignements ainsi recueillis peuvent concerner aussi bien le contenu d'une communication que les données qui s'y rapportent (par exemple, les données qui permettent de

savoir comment, quand et entre quelles adresses la communication électronique s'est déroulée). Ils peuvent être interceptés lors de leur transmission par voie aérienne – généralement par liaison radio ou par satellite – ou par câble. C'est le fournisseur du service de communication, c'est-à-dire les entreprises de télécommunications, d'Internet, de câble et autres qui fournissent diverses formes de transfert électronique d'informations, qui décide si le signal est transmis par voie aérienne ou par câble. La grande majorité des données pertinentes pour le ROEM sont transmises par câble. On appelle « canal de transmission » le moyen utilisé pour transmettre un ou plusieurs signaux. Sauf indication contraire ci-dessous, la réglementation relative aux activités suédoises de ROEM ne distingue pas le contenu des communications des données de communication qui y sont associées, ni l'acheminement des données par voie aérienne de l'acheminement par câble.

15. Selon la loi relative au renseignement extérieur (*Lagen om försvarsunderrättelseverksamhet*, 2000:130), les activités de renseignement extérieur visent à soutenir la politique étrangère, la politique de défense et la politique de sécurité de la Suède, et à repérer les menaces extérieures qui pèsent sur le pays. Elles doivent aussi contribuer à la participation de la Suède à la coopération internationale en matière de sécurité. En vertu de la loi, elles ne peuvent être menées qu'à l'égard de circonstances extérieures au territoire national (article 1 § 1). Cela n'empêche pas que certaines de ces circonstances extérieures puissent avoir des ramifications en Suède, lorsqu'il s'agit, par exemple, de suivre des opérations d'espionnage d'une puissance étrangère qui visent la Suède (travaux préparatoires sur la modification de la loi relative au renseignement extérieur, prop. 2006/07:63, p. 43).

16. Le gouvernement détermine l'orientation de ces activités. Il décide également quelles autorités sont habilitées à adopter des directives plus détaillées et quelle est l'autorité compétente pour mener des activités de renseignement (article 1 §§ 2 et 3). Il adopte chaque année des directives générales sur l'attribution des tâches. Les activités de renseignement extérieur ne peuvent servir à accomplir des missions de répression ou de prévention des infractions : ces missions relèvent de la compétence des autorités de police, de la Sûreté et d'autres autorités, et elles sont soumises à un cadre juridique distinct. Les autorités qui mènent des activités de renseignement extérieur peuvent toutefois assister les autorités chargées de la répression ou de la prévention des infractions (article 4), par exemple au moyen de la cryptanalyse ou en fournissant une aide technique en matière de sécurité de l'information (travaux préparatoires sur la modification de la loi relative au renseignement extérieur, prop. 2006/07:63, p. 136).

17. La collecte de signaux électroniques est une forme de renseignement extérieur. Elle est encadrée par la loi relative au renseignement d'origine électromagnétique (*Lagen om signalspaning i*

försvarsunderrättelseverksamhet, 2008:717), entrée en vigueur le 1er janvier 2009. Cette loi a été modifiée à plusieurs reprises, le 1er décembre 2009, le 1er janvier 2013, le 1er janvier 2015 et le 15 juillet 2016. L'ordonnance relative au renseignement d'origine électromagnétique (*Förordningen om signalspaning i försvarsunderrättelseverksamhet*, 2008:923) contient des dispositions complémentaires. La législation autorise l'Institut national de la défense radio (*Försvarets radioanstalt*, « le FRA ») à mener des activités de ROEM (article 2 de l'ordonnance se rapportant à l'article 1 de la loi).

18. Au cours de ces activités, toutes les communications avec l'étranger transmises par câble sont transférées vers certains points de collecte. Aucune information n'est stockée dans ces points de collecte, et une partie limitée du trafic de données est transférée au FRA par les canaux de transmission (rapport de la commission parlementaire SOU 2016:45, p. 107).

19. Le FRA ne peut mener d'activités de ROEM dans le domaine du renseignement extérieur qu'en vertu d'une directive détaillée d'attribution de tâches émanant du gouvernement, des services gouvernementaux, des forces armées ou, depuis janvier 2013, de la Sûreté ou de la direction des opérations nationales de l'autorité de police (*Nationella operativa avdelningen i Polismyndigheten*, « la NOA ») conformément aux besoins précis du demandeur en termes de renseignement (articles 1 § 1 et 4 § 1 de la loi). En revanche, en vertu de l'article 4 § 2 de la loi, seul le gouvernement est compétent pour orienter les « activités de développement » du FRA. Une directive détaillée d'attribution de tâches détermine l'orientation des activités de renseignement. Cette directive peut concerner une situation ou un phénomène précis mais elle ne peut cibler uniquement une personne physique déterminée (article 4 § 3 de la loi).

20. La compétence pour adopter des directives détaillées d'attribution de tâches conférée à la Sûreté et à la NOA vise à renforcer leur aptitude à obtenir des données de niveau stratégique sur des circonstances extérieures au territoire national concernant le terrorisme international ou d'autres formes graves de criminalité internationale risquant de menacer des intérêts nationaux essentiels. Lorsque ces nouvelles dispositions ont été adoptées, le gouvernement a déclaré, dans les travaux préparatoires (prop. 2011/12:179, p. 19), que le mandat accordé à ces autorités était conforme à l'interdiction de recourir à des activités de ROEM pour accomplir des missions de répression ou de prévention des infractions.

21. En vertu de l'ordonnance relative au renseignement extérieur (*Förordningen om försvarsunderrättelseverksamhet*, 2000:131), toute directive détaillée d'attribution de tâches doit indiquer i) de quelle autorité elle émane, ii) de quelle partie de la directive gouvernementale annuelle sur l'attribution des tâches elle relève, iii) quels sont le phénomène ou la situation visés, et iv) quels sont les besoins en matière de renseignement sur ce phénomène ou cette situation auxquels il faut répondre (article 2a).

B. Le champ d'application du ROEM

22. La loi relative au renseignement d'origine électromagnétique (article 1 § 2) énonce les buts dans lesquels des signaux électroniques peuvent être interceptés dans le cadre d'activités de renseignement extérieur. Elle dispose ainsi qu'il ne peut être mené d'activités de ROEM qu'afin de recueillir des informations :

1. sur des menaces militaires extérieures pesant sur le pays ;
2. sur les conditions de la contribution de la Suède à des missions internationales humanitaires ou de maintien de la paix ou sur les menaces qui pourraient peser sur des intérêts suédois dans le cadre de telles opérations ;
3. sur le contexte stratégique en matière de terrorisme international ou d'autres formes graves de criminalité transfrontière risquant de menacer des intérêts nationaux essentiels ;
4. sur le développement et la prolifération d'armes de destruction massive, d'équipements militaires ou d'autres produits similaires déterminés ;
5. sur des risques extérieurs menaçant gravement l'infrastructure sociale ;
6. sur des conflits à l'étranger susceptibles d'avoir des répercussions sur la sécurité internationale ;
7. sur des opérations de services de renseignement étrangers dirigées contre des intérêts suédois ; et
8. sur les actes ou les intentions d'une puissance étrangère qui revêtent une importance particulière pour la politique étrangère, la politique de défense ou la politique de sécurité de la Suède.

23. Ces huit buts sont détaillés dans les travaux préparatoires de la loi (prop. 2008/09:201, pp. 108-109) :

> « Les buts dans lesquels il est possible d'autoriser une activité de renseignement d'origine électromagnétique sont énumérés en huit points. Le premier point concerne les menaces militaires extérieures pesant sur le pays. Ces menaces ne consistent pas seulement en des menaces imminentes telles des menaces d'invasion, elles peuvent aussi englober des phénomènes susceptibles de se transformer, à long terme, en menaces pour la sécurité. Le libellé de cette disposition inclut donc la collecte d'informations sur le potentiel et les capacités militaires de nos voisins.
>
> Le deuxième point concerne à la fois la collecte des informations nécessaires pour permettre de décider sur une base solide de participer ou non à des missions internationales humanitaires ou de maintien de la paix et la collecte, au cours de telles missions, d'informations concernant des menaces pesant sur le personnel suédois ou sur d'autres intérêts suédois.
>
> Le troisième point concerne la collecte d'informations stratégiques sur le terrorisme international ou d'autres formes graves de criminalité transfrontière, telles que le trafic de stupéfiants ou la traite d'êtres humains, susceptibles par leur échelle de menacer d'importants intérêts nationaux. L'objet du renseignement d'origine électromagnétique portant sur des activités de ce type est d'examiner leurs

implications en termes de politique étrangère et de politique de sécurité. Les activités de renseignement nécessaires à la lutte opérationnelle contre l'activité criminelle relèvent principalement de la compétence de la police.

Le quatrième point concerne la nécessité de recourir au renseignement d'origine électromagnétique pour surveiller, notamment, les activités pertinentes dans le cadre des engagements de la Suède en matière de non-prolifération et de contrôle des exportations, même si elles ne constituent pas une infraction et ne contreviennent à aucune convention internationale.

Le cinquième point inclut, notamment, les menaces informatiques graves provenant de l'étranger. Par menaces graves, on entend celles qui, par exemple, sont dirigées contre des structures publiques essentielles pour l'approvisionnement en énergie et en eau, pour la communication ou pour les services monétaires.

Le sixième point concerne l'analyse des conflits, entre d'autres pays ou dans d'autres pays, susceptibles d'avoir des répercussions sur la sécurité internationale. Il peut s'agir d'actes de guerre habituels entre des États mais aussi de conflits internes ou transfrontaliers entre différents groupes ethniques, religieux ou politiques. Cette analyse comprend l'examen des causes et des conséquences de ces conflits.

Le septième point signifie que le renseignement électromagnétique peut permettre de recueillir des informations sur des activités de renseignement menées contre les intérêts suédois.

Le huitième point offre la possibilité de mener des activités de renseignement d'origine électromagnétique contre des puissances étrangères et leurs représentants afin de recueillir des informations sur leurs intentions ou leurs actes qui revêtent une importance particulière pour la politique étrangère, la politique de défense ou la politique de sécurité de la Suède. Ces activités ne peuvent concerner que ceux qui représentent une puissance étrangère. La condition de l'« importance particulière » permet de souligner qu'il ne suffit pas que le phénomène soit d'intérêt général mais qu'il faut que les renseignements aient un impact direct sur les actes ou les positions de la Suède dans différents domaines de la politique étrangère, de la politique de sécurité ou de la politique de défense. (...) »

24. Le FRA peut également intercepter des signaux électroniques pour se tenir informé des modifications de l'environnement électromagnétique international, des progrès techniques et de la protection des signaux, et pour mettre au point la technologie nécessaire au ROEM (article 1 § 3). Il s'agit là d'« activités de développement » qui, selon les travaux préparatoires (prop. 2006/07:63, p. 72), ne donnent lieu à aucun rapport de renseignement. Les signaux interceptés dans le contexte des activités de développement du FRA n'intéressent pas les autorités pour les données qu'ils peuvent contenir mais uniquement pour la possibilité d'analyser les systèmes et les voies par lesquels ces informations sont transmises. Le FRA peut partager avec d'autres autorités l'expérience acquise sur des questions technologiques. Les activités de développement ne portent généralement pas sur les communications entre individus, quoique des informations sur l'identité d'individus puissent être interceptées.

25. Les activités de ROEM menées sur les données transmises par câble ne peuvent concerner que les signaux traversant la frontière suédoise par des

câbles appartenant à un fournisseur de services de communication (article 2). Les communications entre un émetteur et un destinataire qui se trouvent tous deux en Suède ne peuvent pas être interceptées, que la transmission ait lieu par la voie aérienne ou par câble. Si ces signaux ne peuvent être séparés au point de collecte, l'enregistrement ou les notes les concernant doivent être détruits dès qu'il apparaît qu'ils ont été collectés (article 2a).

26. L'interception des signaux transmis par câble est automatisée et ne doit porter que sur les signaux qui ont été sélectionnés par l'application de sélecteurs (ou « termes de recherche »). On applique aussi une recherche par sélecteurs pour sélectionner les signaux transmis par voie aérienne, si la procédure est automatisée. Les sélecteurs doivent être formulés de manière à limiter autant que possible les atteintes à l'intégrité personnelle. Les sélecteurs se rapportant directement à une personne physique donnée ne peuvent être utilisés que si cela revêt une importance exceptionnelle pour les activités de renseignement (article 3).

27. Les travaux préparatoires de la loi relative au renseignement d'origine électromagnétique (prop. 2006/07:63, p. 90) précisent que l'exigence d'une importance exceptionnelle au sens de l'article 3 découle du fait que l'utilisation de termes de recherche qui se rapportent à une personne donnée, tels que noms patronymiques, numéros de téléphone, adresses de courrier électronique ou adresses IP, comporte des risques particuliers du point de vue du respect de la vie privée. L'utilisation de tels termes de recherche ne devrait être envisagée que dans des circonstances particulières, et elle devrait être précédée d'un examen approfondi de la question de savoir si elle est nécessaire, et notamment si elle est justifiée par l'importance des informations qu'elle permettrait d'obtenir. L'exemple – hypothétique – donné dans les travaux préparatoires est celui d'une crise nationale provoquée par une attaque informatique dirigée contre des systèmes d'une importance cruciale pour la société, qui requerrait que des mesures soient prises immédiatement pour en identifier les acteurs individuels.

28. Une fois les signaux interceptés, ils sont traités, ce qui signifie qu'ils font, par exemple, l'objet d'une cryptanalyse ou d'une traduction. Les informations sont ensuite analysées et rapportées à l'autorité qui a confié au FRA la mission de recueillir les renseignements en question.

29. Le processus, tel que décrit par le gouvernement défendeur, comprend les six étapes suivantes :

1. Les secteurs de l'environnement du ROEM jugés les plus pertinents pour la collecte à un moment donné sont choisis.
2. Des sélecteurs sont appliqués automatiquement aux signaux électroniques dans les secteurs identifiés comme les plus pertinents afin d'intercepter et de réduire progressivement les données recueillies.

3. Les données font ensuite l'objet d'un traitement automatique et manuel qui peut prendre la forme, par exemple, d'une cryptanalyse, d'une structuration et d'une traduction.
4. Les informations traitées sont analysées par un spécialiste dont la tâche consiste à identifier les renseignements parmi les informations disponibles.
5. Un rapport est rédigé et communiqué aux destinataires désignés du renseignement extérieur.
6. Enfin, les personnes concernées sont tenues de faire part de leurs commentaires sur l'utilisation et l'incidence des renseignements fournis et ces commentaires sont transmis aux personnes impliquées dans le processus.

C. L'autorisation de mener des activités de ROEM

30. Le FRA doit demander une autorisation au tribunal pour le renseignement extérieur (*Försvarsunderrättelsedomstolen*) pour toutes les activités de ROEM, y compris les activités de développement. La demande doit contenir l'ordre de mission reçu par le FRA ainsi que des informations sur la directive détaillée d'attribution de tâches dont relève la mission et sur la nécessité des renseignements recherchés. De plus, les canaux de transmission auxquels le FRA demande à avoir accès doivent être spécifiés, de même que les sélecteurs ou catégories de sélecteurs qui seront utilisés. Enfin, la demande doit indiquer la durée pour laquelle l'autorisation est demandée (article 4a).

31. L'autorisation ne peut être accordée que si la mission est conforme aux dispositions de la loi relative au renseignement extérieur et de la loi relative au renseignement d'origine électromagnétique, si le but visé par l'interception de signaux ne peut être atteint par une ingérence moins importante, s'il y a lieu de penser que la mission permettra d'obtenir des informations dont la valeur est nettement supérieure à l'atteinte à l'intégrité personnelle qu'elle risque de causer, si les sélecteurs ou catégories de sélecteurs sont conformes aux dispositions de la loi relative au renseignement d'origine électromagnétique et si la demande ne concerne pas uniquement une personne physique déterminée (article 5).

32. Si elle est accordée, l'autorisation précise la mission pour laquelle des activités de ROEM peuvent être menées, les canaux de transmission auxquels le FRA aura accès, les sélecteurs ou les catégories de sélecteurs de recherche qui peuvent être utilisés, la durée pendant laquelle elle sera valable et les autres conditions à respecter pour limiter les atteintes à l'intégrité personnelle (article 5a).

33. Le FRA peut lui-même décider d'accorder une autorisation si le fait de demander l'autorisation au tribunal pour le renseignement extérieur risque d'engendrer des délais ou d'autres obstacles susceptibles d'avoir un

impact d'une importance essentielle sur la réalisation de l'un des buts spécifiés de l'activité de ROEM concernée. Il doit alors en informer immédiatement le tribunal. Celui-ci statue sans délai sur l'autorisation ; il peut l'annuler ou la modifier (article 5b).

34. La composition du tribunal pour le renseignement extérieur et ses activités sont régies par la loi sur le tribunal pour le renseignement extérieur (*Lagen om Försvarsunderrättelsedomstol*, 2009:966). Le tribunal est composé d'un président, d'un ou deux vice-présidents et de deux à six autres membres. Le président est un juge permanent nommé par le gouvernement sur proposition de la commission de proposition des juges (*Domarnämnden*). Les vice-présidents, qui doivent avoir une formation juridique et une expérience préalable en tant que juges, et les autres membres, qui doivent avoir des connaissances spécialisées pertinentes pour l'activité du tribunal, sont nommés par le gouvernement pour un mandat de quatre ans. Les demandes d'autorisation d'activités de ROEM sont examinées au cours d'une audience, qui peut se tenir à huis clos s'il apparaît clairement que la tenue d'une audience publique risquerait d'aboutir à la divulgation d'informations classées secrètes. Pendant l'examen de la demande par le tribunal, le FRA ainsi qu'un représentant chargé de la protection de la vie privée (*integritesskyddsombud*) sont présents. Ledit représentant, qui ne représente pas une personne en particulier mais les intérêts des individus en général, repère les aspects problématiques du point de vue du respect de la vie privée ; il a accès au dossier de l'affaire et peut faire des déclarations. Les représentants chargés de la protection de la vie privée sont nommés par le gouvernement pour un mandat de quatre ans ; ils doivent être ou avoir été juges permanents ou avocats. Le tribunal ne peut tenir une audience et statuer sur une demande en l'absence d'un représentant que si l'urgence de l'affaire est telle qu'un retard compromettrait gravement la réalisation du but de la demande. Les décisions du tribunal sont définitives.

D. La durée des activités de ROEM

35. L'autorisation peut être accordée pour une période déterminée d'une durée maximale de six mois. Après réexamen, elle peut être prolongée par périodes de six mois (article 5a de la loi relative au renseignement d'origine électromagnétique).

E. Les procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation et la destruction des données interceptées

36. L'Inspection du renseignement extérieur (*Statens inspektion för försvarsunderrättelseverksamheten* (SIUN), paragraphes 50-54 ci-dessous) supervise l'accès aux canaux de transmission. Les fournisseurs de services

de communication sont tenus de transférer les signaux traversant la frontière suédoise par câble vers des « points de collaboration » convenus avec l'Inspection. Celle-ci donne au FRA l'accès aux canaux de transmission dans la mesure permise par l'autorisation de ROEM, en application de l'autorisation délivrée par le tribunal pour le renseignement extérieur (chapitre 6, article 19a de la loi sur les communications électroniques (*Lagen om elektronisk kommunikation*, 2003:389)). Le Conseil de législation (*Lagrådet*), organe qui émet, à la demande du gouvernement ou d'une commission parlementaire, des avis sur certains projets de loi, a estimé que le simple fait que l'État puisse avoir accès aux télécommunications constitue déjà une atteinte à la vie privée et au respect de la correspondance (prop. 2006/07:63, p. 172).

37. En vertu de la loi relative au renseignement d'origine électromagnétique, les données interceptées doivent être immédiatement détruites par le FRA si i) elles concernent une personne physique déterminée et revêtent une faible importance pour le ROEM, ii) elles sont protégées par les dispositions constitutionnelles relatives au secret protégeant l'anonymat des auteurs et des sources journalistiques, iii) elles contiennent des informations échangées entre un suspect et son avocat et sont donc protégées par le principe de la confidentialité des échanges entre l'avocat et son client, ou si iv) elles contiennent des informations données dans un contexte religieux (confession ou conseil individuel), sauf raisons exceptionnelles justifiant leur examen (article 7).

38. Si, malgré l'interdiction de telles interceptions, des communications entre un émetteur et un destinataire qui se trouvent tous deux en Suède ont été interceptées, celles-ci doivent être détruites dès qu'il apparaît qu'il s'agit de communications intérieures (article 2a).

39. Si une autorisation accordée en urgence par le FRA (paragraphe 21 ci-dessus) est annulée ou modifiée par le tribunal pour le renseignement extérieur, tous les renseignements recueillis par des moyens qui ne sont dès lors plus autorisés doivent immédiatement être détruits (article 5b § 3).

40. La loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA (*Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, 2007:259) contient des dispositions sur le traitement des données personnelles dans le domaine du ROEM. Entrée en vigueur le 1er juillet 2007, elle a été modifiée le 30 juin 2009 puis le 15 février 2010 et le 1er mars 2018. Elle a pour objet de garantir une protection contre les atteintes à l'intégrité personnelle (chapitre 1, article 2). Le FRA doit notamment veiller à ce que les données personnelles ne soient collectées que dans des buts expressément indiqués et justifiés. Ces buts sont déterminés soit par l'orientation des activités de renseignement extérieur qui est donnée par une directive détaillée d'attribution de tâches, soit par ce qui est nécessaire pour suivre l'évolution de l'environnement

électromagnétique, des progrès techniques et de la protection des signaux. Les données personnelles traitées doivent également être adéquates et pertinentes au regard de la finalité du traitement. Il ne peut être traité plus de données personnelles que celles nécessaires pour atteindre le but visé. Toutes les mesures raisonnables doivent être prises pour corriger, bloquer et détruire les données personnelles incorrectes ou incomplètes (chapitre 1, articles 6, 8 et 9).

41. Les données à caractère personnel ne doivent pas être traitées uniquement à raison des informations connues concernant la race ou l'origine ethnique de la personne, ses convictions politiques, religieuses ou philosophiques, son appartenance à un syndicat, son état de santé ou sa sexualité. Toutefois, lorsque des données personnelles sont traitées pour une raison différente, ce type d'information peut être utilisé si cela est absolument nécessaire aux fins du traitement. Les informations concernant l'apparence physique d'une personne doivent toujours être formulées de manière objective et respectueuse de la dignité humaine. Les recherches de renseignements ne peuvent utiliser les indicateurs personnels susmentionnés comme sélecteurs que si cela est absolument nécessaire aux fins de la réalisation du but dans lequel la recherche est menée (chapitre 1, article 11).

42. Les employés du FRA qui traitent des données à caractère personnel sont soumis à une procédure officielle d'habilitation de sécurité et à une obligation de confidentialité quant aux données couvertes par le secret. Ils s'exposent à des sanctions pénales en cas de faute dans le traitement de ces données (chapitre 6, article 2).

43. Les données à caractère personnel soumises à un traitement automatisé doivent être détruites dès qu'elles ne sont plus nécessaires (chapitre 6, article 1).

44. L'ordonnance sur le traitement des données à caractère personnel dans le cadre des activités du FRA (*Förordningen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, 2007:261) contient d'autres dispositions en la matière. Elle prévoit notamment que le FRA peut tenir des bases de données brutes contenant des informations à caractère personnel. Les données brutes sont des informations non traitées qui ont été recueillies par traitement automatisé. Les données à caractère personnel contenues dans ces bases de données doivent être détruites dans un délai d'un an à compter de la date à laquelle elles ont été collectées (article 2).

F. Les conditions dans lesquelles les données interceptées peuvent être communiquées à d'autres parties

45. Les renseignements recueillis doivent être rapportés aux autorités concernées conformément aux dispositions de la loi relative au

renseignement extérieur (article 8 de la loi relative au renseignement d'origine électromagnétique).

46. Les services gouvernementaux, les forces armées, la Sûreté, la NOA, l'Inspection des produits stratégiques (*Inspektionen för strategiska produkter*), l'administration du matériel de défense (*Försvarets materialverk*), l'Institut de recherche sur la défense (*Totalförsvarets forskningsinstitut*), le service de la protection civile (*Myndigheten för samhällsskydd och beredskap*) et le service national des douanes (*Tullverket*) peuvent avoir un accès direct aux rapports de renseignement établis dans la mesure décidée par le FRA (article 9 de l'ordonnance sur le traitement des données à caractère personnel dans le cadre des activités du FRA). Cependant, à ce jour, le FRA n'a accordé d'accès direct à aucun d'entre eux.

47. Le FRA peut également donner à la Sûreté et aux forces armées un accès direct à des données qui constituent des résultats d'analyse dans le cadre d'une collecte de données pour analyse et dont les autorités ont besoin pour faire des évaluations stratégiques de la menace terroriste qui pèse sur la Suède et les intérêts suédois (chapitre 1, article 15 de la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA, et article 13a de l'ordonnance).

48. Selon les travaux préparatoires (prop 2017/18:36), ce dernier type d'accès peut être accordé par le FRA dans le cadre d'une collaboration qu'il entretient avec la Sûreté et les forces armées au sein d'un groupe de travail, le Centre national d'évaluation des menaces terroristes (*Nationellt centrum för terrorhotbedömning* ; « le NCT »), dans lequel un certain nombre d'analystes provenant de ces trois autorités travaillent ensemble et rédigent des rapports contenant des évaluations stratégiques des menaces terroristes. Les analystes du NCT ont ainsi accès, avec la permission du FRA et pour autant que ces données sont pertinentes pour pareilles évaluations, à des « résultats d'analyse » contenus dans les bases de données du FRA. Les analystes n'ont toutefois pas un accès direct aux bases de données du FRA pour y effectuer des recherches librement. Par ailleurs, même si les informations auxquelles ils ont ainsi directement accès peuvent contenir des données à caractère personnel, les analystes du NCT se livrent à des évaluations de nature stratégique et générale qui ne portent pas sur des individus.

49. Les données à caractère personnel ne peuvent être communiquées à d'autres États ou à des organisations internationales que si le secret ne s'y oppose pas et si cette communication est nécessaire pour que le FRA puisse exercer ses activités de coopération internationale en matière de défense et de sécurité. Le gouvernement peut également décider, à titre général ou dans un cas particulier, d'autoriser cette communication de données à caractère personnel dans d'autres cas lorsqu'elle est nécessaire pour les activités du FRA (chapitre 1, article 17 de la loi sur le traitement des

données à caractère personnel dans le cadre des activités du FRA). Le FRA peut divulguer des données à caractère personnel à une autorité étrangère ou à une organisation internationale si cette communication est bénéfique pour la gestion de l'État suédois (*statsledningen*) ou pour la stratégie de défense globale de la Suède (*totalförsvaret*). Les informations ainsi communiquées ne doivent pas nuire aux intérêts suédois (article 7 de de l'ordonnance sur le traitement des données à caractère personnel dans le cadre des activités du FRA).

G. La supervision de l'application des mesures de ROEM

50. La loi relative au renseignement extérieur (article 5) et la loi relative au renseignement d'origine électromagnétique (article 10) prévoient qu'une autorité doit superviser les activités de renseignement extérieur en Suède et vérifier que les activités du FRA respectent les dispositions de la loi relative au renseignement d'origine électromagnétique. L'autorité de supervision – l'Inspection du renseignement extérieur – est notamment chargée de contrôler l'application de la loi relative au renseignement extérieur et de l'ordonnance qui y est associée, et de vérifier que les activités de renseignement extérieur sont menées conformément aux directives applicables (article 4 de l'ordonnance portant instructions pour l'Inspection du renseignement extérieur (*Förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*, 2009:969)). Elle contrôle aussi le respect de la loi relative au renseignement d'origine électromagnétique, en vérifiant, en particulier, les sélecteurs employés, la destruction des renseignements et la communication des rapports. Si une inspection révèle qu'une collecte de renseignements n'a pas respecté l'autorisation sur laquelle elle était fondée, l'Inspection peut décider de mettre fin à l'opération correspondante ou ordonner la destruction des renseignements ainsi recueillis (article 10 de la loi relative au renseignement d'origine électromagnétique). Le FRA doit signaler à l'Inspection les sélecteurs qui visent directement une personne physique déterminée (article 3 de l'ordonnance relative au renseignement d'origine électromagnétique).

51. L'Inspection du renseignement extérieur est dirigée par un conseil dont les membres sont nommés par le gouvernement pour un mandat d'au moins quatre ans. Le président et le vice-président doivent être ou avoir été juges permanents. Les autres membres sont choisis parmi les candidats proposés par les groupes parlementaires (article 10 § 3 de la loi relative au renseignement d'origine électromagnétique).

52. Tous les avis et toutes les propositions de mesures formulés par l'Inspection à l'issue d'une inspection sont transmis au FRA et, si nécessaire, au gouvernement. L'Inspection remet également au gouvernement des rapports annuels sur ses inspections (article 5 de

l'ordonnance portant instructions pour l'Inspection du renseignement extérieur), qui sont rendus publics. Par ailleurs, elle informe le ministère public (*Åklagarmyndigheten*) de toute infraction potentielle et, si elle découvre des irrégularités susceptibles d'engager la responsabilité de l'État, elle remet un rapport au chancelier de la Justice (*Justitiekanslern*). Un rapport peut également être remis à l'autorité de protection des données (*Datainspektionen*), qui est l'autorité de supervision du traitement par le FRA des données à caractère personnel (article 15).

53. De 2009, année de sa création, à 2017, l'Inspection a mené au total 102 inspections, qui ont abouti à la remise de 15 avis au FRA et d'un avis au gouvernement. Aucune inspection n'a révélé de raisons de mettre fin à une collecte de renseignements ou d'en détruire les résultats. Il ressort des brèves descriptions contenues dans les rapports annuels de l'Inspection qu'au cours de ses inspections celle-ci a procédé à de nombreuses vérifications détaillées des sélecteurs employés, de la destruction des renseignements, de la communication des rapports, du traitement des données personnelles et du respect général de la législation, des directives et des autorisations relatives aux activités de ROEM. Entre 2010 et 2014, l'utilisation des sélecteurs a ainsi été inspectée à dix-sept reprises et a donné lieu à un avis et à une proposition de modification des procédures de traitement du FRA. Au cours de la même période, la destruction de données relatives à des activités de ROEM a été contrôlée à neuf reprises et a donné lieu en 2011 à un avis par lequel l'Inspection invitait le FRA à modifier son règlement interne, ce qui a été fait la même année. En 2011, l'Inspection a également vérifié si les collectes de données menées par le FRA pour d'autres États l'avaient été conformément au droit applicable. Aucun avis n'a ensuite été délivré. Une inspection effectuée en 2014 a porté sur un contrôle général de la coopération du FRA en matière de renseignement avec d'autres États et avec des organisations internationales. Elle n'a donné lieu à aucun avis ni aucune suggestion au FRA. En 2015 et 2016, un examen global du respect des limitations fixées par les autorisations délivrées par le tribunal pour le renseignement extérieur a donné lieu à un avis. En 2016 et 2017, l'Inspection a procédé à une vérification détaillée du traitement par le FRA des données à caractère personnel, et plus particulièrement des données personnelles sensibles relatives à des éléments stratégiques concernant le terrorisme international ou d'autres formes graves de criminalité transfrontière menaçant des intérêts nationaux importants. Elle n'a formulé aucun avis ni aucune suggestion. Toutefois, la même année, elle a remis un avis au gouvernement à la suite d'une inspection visant à déterminer si les activités de renseignement du FRA avaient été menées conformément à l'orientation définie. Au cours de la période 2009-2017, elle a constaté en une occasion la présence d'un motif de remettre un rapport à une autre autorité – l'autorité de protection des données –, au sujet de l'interprétation d'une disposition de loi. Dans ses

rapports annuels, elle a indiqué qu'elle avait eu accès à toutes les informations nécessaires à ses inspections.

54. Les activités de supervision de l'Inspection du renseignement extérieur ont été vérifiées par la Direction nationale du contrôle de la gestion publique (*Riksrevisionen*), autorité placée sous la tutelle du parlement. Dans un rapport publié en 2015, celle-ci a constaté que le FRA avait mis en place des procédures pour traiter les avis émis par l'Inspection et que la supervision que celle-ci exerçait avait contribué au développement des activités du FRA. Elle a également observé que les suggestions avaient été traitées avec sérieux et qu'elles avaient donné lieu, si nécessaire, à des réformes. Elle a relevé qu'à l'exception d'un cas où il a déféré la question au gouvernement, le FRA a toujours pris les mesures décidées par l'Inspection. Elle a toutefois estimé que les inspections n'étaient pas assez documentées et qu'il aurait fallu qu'elles visent des buts clairement définis.

55. Au sein du FRA, il existe un conseil de protection de la vie privée chargé de contrôler en permanence les mesures prises pour garantir la protection de l'intégrité personnelle. Ce conseil, dont les membres sont nommés par le gouvernement, communique ses observations à la direction du FRA ou, en présence de motifs le justifiant, à l'Inspection (article 11 de la loi relative au renseignement d'origine électromagnétique).

56. La loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA contient d'autres dispositions relatives à la supervision. Le FRA doit désigner un ou plusieurs délégués à la protection des données et en informer l'autorité de protection des données (chapitre 4, article 1). Le délégué à la protection des données est chargé de vérifier de manière indépendante que le FRA administre les données personnelles de manière légale et appropriée, et de signaler toute irrégularité qu'il constaterait. S'il soupçonne certaines irrégularités et qu'aucune correction n'y est apportée, il doit présenter un rapport à l'autorité de protection des données (chapitre 4, article 2).

57. L'autorité de protection des données, qui est placée sous l'autorité du gouvernement, peut si elle le demande accéder aux données à caractère personnel traitées par le FRA et aux documents relatifs au traitement des données à caractère personnel, ainsi qu'aux mesures de sécurité prises à cet égard. Elle peut accéder également aux lieux où les données personnelles sont traitées (chapitre 5, article 2). Si elle constate que des données à caractère personnel sont traitées de manière illégale ou pourraient l'être, elle doit essayer d'y remédier en communiquant ses observations au FRA (chapitre 5, article 3). Elle peut également saisir le tribunal administratif (*förvaltningsrätten*) de Stockholm pour obtenir la destruction des données personnelles traitées de manière illégale (chapitre 5, article 4). Selon des copies de courriers électroniques échangés entre la requérante et le tribunal administratif en avril 2019, il n'existerait aucune trace dans les registres

électroniques de cette juridiction d'une demande de l'autorité de protection des données en ce sens.

H. La notification des mesures de surveillance secrète

58. En vertu de la loi relative au renseignement d'origine électromagnétique, lorsqu'il a employé des sélecteurs visant directement une personne physique déterminée, le FRA est tenu d'en aviser l'intéressé, en précisant la date et le but des mesures, et ce dès qu'il est possible de le faire sans risquer de nuire aux activités de renseignement extérieur, mais au plus tard un mois après la fin de la mission de ROEM (article 11a).

59. La notification peut toutefois être différée si le secret l'exige, en particulier en cas de secret lié à la défense ou à la protection de relations internationales. Si, en raison du secret, la personne concernée n'a pas été avisée de la surveillance dans un délai d'un an à compter de la fin de la mission, il n'est plus nécessaire de l'en informer. Par ailleurs, aucune notification n'est nécessaire si les mesures ne concernent que la situation d'une puissance étrangère ou les relations entre des puissances étrangères (article 11b).

60. Dans son rapport de 2010, l'autorité de protection des données a noté, entre autres, qu'en raison du secret la procédure de notification aux particuliers n'avait jamais été utilisée par le FRA (paragraphe 75 ci-dessous).

I. Les recours

61. La loi relative au renseignement d'origine électromagnétique prévoit que toute personne, quels que soient sa nationalité et son lieu de résidence, peut saisir l'Inspection du renseignement extérieur. Celle-ci doit alors rechercher si les communications de cette personne ont été interceptées dans le cadre d'activités de ROEM et, si tel a été le cas, vérifier si l'interception et le traitement des informations correspondantes ont été effectués dans le respect du droit applicable. Elle doit informer le demandeur qu'elle a procédé au contrôle sollicité (article 10a). Toute personne physique ou morale peut présenter une demande, quels que soient sa nationalité et son lieu de résidence. Au cours de la période 2010-2017, 132 demandes ont été traitées et aucune irrégularité n'a été établie. En 2017, dix demandes ont été traitées, contre quatorze en 2016. Les décisions rendues par l'Inspection sur les demandes dont elle est saisie sont définitives.

62. En vertu de la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA, celui-ci est également tenu de fournir des informations lorsqu'il en reçoit la demande. Toute personne peut demander une fois par année civile si des données à caractère personnel la concernant sont en cours de traitement ou ont été traitées. Si tel est le cas, le

FRA doit préciser les informations qu'il détient sur la personne en question, la source de leur collecte, la finalité de leur traitement et les destinataires ou catégories de destinataires auxquels les données personnelles sont ou ont été communiquées. Ces informations doivent normalement être fournies dans un délai d'un mois à compter de la demande (chapitre 2, article 1). Ce droit à l'information ne s'applique toutefois pas si le secret fait obstacle à la divulgation des éléments en question (chapitre 2, article 3).

63. À la suite d'une demande formulée par une personne dont des données à caractère personnel ont été enregistrées, le FRA doit rapidement corriger, bloquer ou détruire les données qui n'ont pas été traitées conformément à la loi. Il doit également aviser tout tiers qui a reçu les données si la personne en fait la demande ou si cette notification est de nature à permettre d'éviter un préjudice ou un inconvénient importants. La notification n'est cependant pas nécessaire si elle est impossible ou si elle requerrait un effort disproportionné (chapitre 2, article 4).

64. Les décisions du FRA sur la divulgation et les mesures correctives concernant des données à caractère personnel peuvent faire l'objet d'un recours devant le tribunal administratif de Stockholm (chapitre 6, article 3). Selon des copies de courriers électroniques échangés entre la requérante et le tribunal administratif en avril 2019, il n'existerait aucune trace dans les registres électroniques de cette juridiction de l'exercice d'un tel recours.

65. L'État est responsable des dommages résultant de la violation de l'intégrité personnelle causée par un traitement des données personnelles non conforme à la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA (chapitre 2, article 5). Les demandes d'indemnisation doivent être présentées au chancelier de la Justice.

66. Outre les recours indiqués ci-dessus, établis par la législation relative au renseignement d'origine électromagnétique, le droit suédois prévoit plusieurs autres moyens de contrôle et mécanismes de plainte. Les médiateurs parlementaires (*Justititeombudsmannen*) supervisent l'application des lois et des règlements dans les activités publiques. À leur demande, les tribunaux et autorités sont tenus de produire des informations et des avis (chapitre 13, article 6 de l'Instrument de gouvernement – *Regeringsformen*), et notamment de leur donner accès à des procès-verbaux et à d'autres documents. Les médiateurs doivent en particulier vérifier que les tribunaux et autorités respectent les dispositions de l'Instrument de gouvernement relatives à l'objectivité et à l'impartialité et que les activités publiques ne portent pas atteinte aux droits et libertés fondamentaux des citoyens (article 3 de la loi portant instructions pour les médiateurs parlementaires – *Lagen med instruktion för Riksdagens ombudsmän*, 1986:765). La supervision, à laquelle sont soumis le tribunal pour le renseignement extérieur et le FRA, s'exerce par l'examen des plaintes du public et par des inspections et des enquêtes (article 5). L'examen se conclut par une décision dans laquelle le médiateur rend un avis, qui n'est pas

juridiquement contraignant, sur le point de savoir si le tribunal ou l'autorité a enfreint la loi ou agi de manière fautive ou inappropriée. Le médiateur peut également engager une procédure pénale ou disciplinaire contre un agent public qui a commis une infraction pénale ou manqué à ses devoirs en ne respectant pas les obligations liées à sa fonction (article 6).

67. Disposant d'un mandat similaire à celui des médiateurs parlementaires, le chancelier de la Justice contrôle le respect par les agents de l'administration publique des lois et règlements et de leurs obligations (article 1 de la loi sur la supervision assurée par le chancelier de la Justice – *Lagen om justitiekanslerns tillsyn*, 1975:1339). Pour ce faire, il examine les plaintes individuelles ou mène des inspections et des enquêtes, par exemple sur le tribunal pour le renseignement extérieur et le FRA. Selon des copies de courriers électroniques échangés entre la requérante et le bureau du chancelier de la Justice en avril 2019, douze plaintes lui auraient été adressées en 2008 et une seule en 2013. Après examen, aucune d'entre elles n'a été jugée comme nécessitant une action.

68. À la demande du chancelier, les tribunaux et autorités sont tenus de produire des informations et des avis et de donner accès à des procès-verbaux et à d'autres documents (articles 9 et 10). Les décisions du chancelier de la Justice sont de même nature que celles des médiateurs parlementaires, notamment en ce qu'elles ne sont pas juridiquement contraignantes. Cependant, par tradition, les avis du chancelier et des médiateurs suscitent un grand respect dans la société suédoise et ils sont généralement suivis (*Segerstedt-Wiberg et autres c. Suède*, n° 62332/00, § 118, CEDH 2006-VII). Le chancelier a la même compétence que les médiateurs pour engager des procédures pénales ou disciplinaires (articles 5 et 6).

69. Le chancelier de la Justice peut également statuer sur les plaintes et les demandes d'indemnisation dirigées contre l'État, notamment sur celles fondées sur une violation alléguée de la Convention. La Cour suprême et le chancelier de la Justice ont élaboré ces dernières années une jurisprudence selon laquelle un principe général du droit permet d'ordonner une indemnisation pour les violations de la Convention même en l'absence de base légale directe en droit interne dans la mesure où la Suède est tenue de réparer toute violation de la Convention en accordant aux victimes un droit à indemnisation (*Lindstrand Partners Advokatbyrå AB c. Suède*, n° 18700/09, §§ 58-62 et 67, 20 décembre 2016, et les références qui y sont citées). Le 1er avril 2018, le droit à réparation pour les violations de la Convention a été inscrit dans la loi grâce à l'adoption d'une nouvelle disposition (chapitre 3, article 4 de la loi sur la responsabilité civile – *Skadeståndslagen*, 1972:207).

70. Outre les fonctions de supervision mentionnées ci-dessus que lui confèrent l'ordonnance portant instructions pour l'Inspection du renseignement extérieur et la loi sur le traitement des données à caractère

personnel dans le cadre des activités du FRA (paragraphes 52, 56 et 57 ci-dessus), l'autorité de protection des données est chargée, de manière générale, de protéger les individus contre les atteintes qui peuvent être portées à l'intégrité personnelle par le traitement des données à caractère personnel, en vertu de la loi portant dispositions complémentaires au règlement général de l'Union européenne sur la protection des données (*Lagen med kompletterande bestämmelser till EU:s dataskyddsförordning*), qui est entrée en vigueur le 25 mai 2018, le même jour que le règlement européen qu'elle complète (paragraphe 94 ci-dessous). En ce qui concerne les activités de ROEM menées par le FRA, la loi sur les données à caractère personnel (*Personuppgiftslagen*, 1998:204) reste applicable, même si elle est remplacée pour le reste par le nouveau règlement européen et la loi qui le complète. Elle confie à l'autorité de protection des données la même mission générale de supervision, dans l'exercice de laquelle l'autorité peut recevoir et examiner des plaintes individuelles.

J. Le secret au FRA

71. La loi sur l'accès du public à l'information et sur le secret (*Offentlighets- och sekretesslagen*, 2009:400) contient une disposition spécifique sur les activités de ROEM menées par le FRA. Le secret s'applique aux informations concernant la situation personnelle ou économique d'une personne, à moins qu'il ne soit évident que ces informations peuvent être divulguées sans que la personne concernée ni aucune autre personne qui lui est étroitement liée ne soit lésée. La présomption est que les informations relèvent du secret (chapitre 38, article 4).

72. En vertu de la loi, le secret s'applique également de manière générale aux activités de renseignement extérieur pour ce qui est des informations concernant un autre État, une organisation internationale, une autorité, un citoyen ou une personne morale d'un autre État, si l'on peut présumer que leur divulgation porterait atteinte aux relations internationales de la Suède ou nuirait au pays d'une autre manière (chapitre 15, article 1).

73. Le secret s'applique par ailleurs aux informations concernant les activités liées à la défense du pays et à la planification de pareilles activités ainsi qu'aux informations liées d'une autre manière à la stratégie de défense globale du pays, si l'on peut présumer que leur divulgation porterait atteinte à la défense du pays ou mettrait en danger la sécurité nationale (chapitre 15, article 2).

74. Les informations couvertes par le secret en vertu de la loi sur l'accès du public à l'information et sur le secret ne peuvent être divulguées à une autorité étrangère ou à une organisation internationale, à moins que i) cette divulgation ne soit autorisée par une disposition de loi expresse (article 7 de l'ordonnance sur le traitement des données à caractère personnel dans le

cadre des activités du FRA), ou que ii) ces informations ne puissent dans une situation analogue être communiquées à une autorité suédoise et que l'autorité qui les divulgue n'estime qu'il est évident que la communication des informations à l'autorité étrangère ou à l'organisation internationale est conforme aux intérêts suédois (chapitre 8, article 3 de la loi).

K. Les rapports de l'autorité de protection des données

75. Le 12 février 2009, le gouvernement ordonna à l'autorité de protection des données d'examiner, du point de vue de l'intégrité, la manière dont le FRA administrait les données à caractère personnel. Dans son rapport, publié le 6 décembre 2010, l'autorité indiqua que ses conclusions étaient globalement positives. Elle nota que le FRA prenait sérieusement en compte les questions relatives au traitement des données à caractère personnel et à l'intégrité personnelle, et qu'afin de réduire le plus possible le risque d'atteintes injustifiées à l'intégrité personnelle, il consacrait un temps et des ressources considérables à la mise en place de procédures et à la formation de son personnel. Elle constata par ailleurs que rien n'indiquait que le FRA manipulât des données à caractère personnel à des fins non autorisées par la législation en vigueur. Elle indiqua toutefois, notamment, qu'il était nécessaire d'améliorer les méthodes visant à distinguer les communications nationales des communications avec l'étranger. À cet égard, elle observa que, même si le FRA avait mis en place des mécanismes dans ce domaine, il n'y avait aucune garantie contre l'interception de communications nationales, et que, même si cela s'était rarement produit, il était déjà arrivé que de telles communications fussent interceptées. Enfin, elle nota qu'en raison du secret la procédure de notification aux particuliers (paragraphes 58-60 ci-dessus) n'avait jamais été utilisée par le FRA.

76. L'autorité de protection des données rendit un deuxième rapport le 24 octobre 2016. À nouveau, elle constata que rien n'indiquait que des données à caractère personnel eussent été collectées dans d'autres buts que ceux assignés aux activités de ROEM. Elle nota également que le FRA vérifiait en permanence si les données interceptées et la surveillance des canaux de transmission à partir desquels il obtenait les renseignements étaient toujours nécessaires à la réalisation de ces buts. Elle constata que par ailleurs rien n'indiquait que les dispositions relatives à la destruction des données à caractère personnel eussent été méconnues (paragraphes 37-39 ci-dessus). Elle reprocha toutefois au FRA une irrégularité qu'elle avait déjà soulignée en 2010, à savoir qu'il ne contrôlait pas suffisamment les journaux d'historique (*logs*) permettant de détecter l'utilisation injustifiée de données à caractère personnel.

L. Le rapport du comité sur le renseignement d'origine électromagnétique

77. Le 12 février 2009, le gouvernement décida également de nommer un comité composé principalement de parlementaires, le comité sur le renseignement d'origine électromagnétique (*Signalspaningskommittén*), chargé de surveiller les activités de ROEM menées par le FRA afin d'en examiner les conséquences pour l'intégrité personnelle. Le 11 février 2011, le comité rendit son rapport (*Uppföljning av signalspaningslagen*, SOU 2011:13). Il avait examiné principalement les activités de ROEM aériennes, car celles concernant les données acheminées par câble n'avaient pas encore commencé à grande échelle.

78. Le comité conclut que les préoccupations relatives à l'intégrité personnelle étaient prises au sérieux par le FRA et qu'elles faisaient partie intégrante de l'élaboration de ses procédures. Il releva toutefois qu'il était difficile en pratique de séparer les communications par câble nationales de celles qui traversaient la frontière suédoise, et que toutes les communications nationales qui n'étaient pas séparées au stade du traitement automatisé l'étaient manuellement au stade du traitement ou de l'analyse. Il observa par ailleurs que les sélecteurs employés pour les données de communication étaient moins spécifiques que ceux utilisés pour l'interception du contenu d'une communication et que, par conséquent, un plus grand nombre de personnes pouvaient voir leurs données conservées par le FRA.

79. Le comité constata également dans son rapport que les activités de développement du FRA (paragraphe 24 ci-dessus) risquaient de conduire à l'interception de communications non pertinentes et éventuellement à leur lecture ou à leur écoute par le personnel du FRA. Il observa toutefois que les activités de développement étaient directement essentielles à la capacité du FRA à mener des activités de ROEM et qu'en outre les informations obtenues dans le cadre des activités de développement ne pouvaient être utilisées dans le cadre des activités ordinaires de renseignement que si cette utilisation était conforme aux buts fixés par la loi et aux directives d'attribution de tâches pertinentes émises pour le ROEM.

80. Tout comme l'autorité de protection des données, le comité souligna qu'en réalité, en raison du secret, l'obligation pour le FRA d'aviser les personnes ayant directement et personnellement fait l'objet de mesures de surveillance secrète était très limitée. Il conclut que cette obligation ne permettait nullement de garantir la sécurité juridique ni d'assurer une protection contre les atteintes à l'intégrité personnelle. Il estima toutefois que la procédure d'autorisation par le tribunal pour le renseignement extérieur des mesures de ROEM (paragraphes 30-34 ci-dessus) et la supervision exercée par l'Inspection du renseignement extérieur (paragraphes 36 et 50-54 ci-dessus) et le conseil de protection de la vie

privée (paragraphe 55 ci-dessus), notamment, offraient une protection importante pour l'intégrité personnelle. Il releva à cet égard que, même si le conseil de protection de la vie privée faisait partie du FRA, il agissait de manière indépendante.

II. LE DROIT INTERNATIONAL PERTINENT

A. Nations unies

81. La Résolution n° 68/167 sur le droit à la vie privée à l'ère du numérique, 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, et son protocole additionnel (STE n° 108)*

82. Cette Convention, qui est entrée en vigueur à l'égard de la Suède le 1er octobre 1985, 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 1 – 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. »

83. Le rapport explicatif de la Convention susmentionnée expose ce qui suit concernant son article 9 :

« 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. (...) »

84. Le Protocole additionnel du 8 novembre 2001 à la Convention du Conseil de l'Europe 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), entré en vigueur pour la Suède le 1er juillet 2004, dispose, en ses parties pertinentes :

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. »

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

85. La Recommandation n° R (95) 4 du Comité des Ministres sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, 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. »

3. 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

86. Dans ce rapport publié en décembre 2015, 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.

87. 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 le *Foreign Intelligence Surveillance Court* (« la Cour FISA »). 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.

88. 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.

89. 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.

90. 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.

91. 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 PERTINENT DE L'UNION EUROPÉENNE

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

92. 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 à caractère personnel

93. 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).

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

95. 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.

96. 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. »

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. »

97. 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 (voir le paragraphe 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)*

98. 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.

99. 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.

100. 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.

101. 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.

102. 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 des 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)

103. Dans l'affaire *Secretary of State for the Home Department contre Tom Watson e.a.*, M. Watson et deux autres personnes avaient sollicité le contrôle juridictionnel de la légalité de l'article 1er de la loi adoptée par le Royaume-Uni en 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 loi de 2000 portant réglementation des pouvoirs d'enquête (*Regulation of Investigatory Powers Act* 2000 – « la RIPA »), ordonner à un opérateur de télécommunications publiques de conserver des données de communication. M. Watson et les deux autres personnes soutenaient notamment que cet article était incompatible avec les articles 7 et 8 de la Charte et avec l'article 8 de la Convention.

104. 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.

105. 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.

106. 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.

107. 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.

108. 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 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)

109. 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.

110. 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. »

111. 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)

112. 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.

113. 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.

114. 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.

115. 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.

116. 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)

117. 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.

118. 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 l'Office national de sécurité américain (*National Security Agency*, « 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.

119. 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.

120. Après examen des activités des services de renseignement américains autorisées par l'article 702 de la de la loi sur la surveillance opérée aux fins du renseignement extérieur (*Foreign Intelligence Surveillance Act*, « la FISA ») et le décret présidentiel n° 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.

121. 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.

122. 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.

123. 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, Secretary of State for the Home Department, Government Communications Headquarters, Security Service et Secret Intelligence Service (affaire 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 C-511/18, C-512/18 et C-520/18 ; ECLI:EU:C:2020:791)

124. Le 8 septembre 2017, le Tribunal anglais des pouvoirs d'enquête (*Investigatory Powers Tribunal*, « 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 communications 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.

125. 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.

126. 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.

127. 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.

128. 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.

129. 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.

130. 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

1. Vue d'ensemble

131. 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.

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

133. Le régime mis en place au Royaume-Uni est détaillé dans l'arrêt rendu par la Cour dans l'affaire *Big Brother Watch et autres c. Royaume-Uni*, nos 58170/13 et 2 autres, le 25 mai 2021.

134. 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 communications 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.

135. 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.

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

136. 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*).

137. 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.

138. L'échange des données interceptées 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.

139. 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.

140. 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.

141. 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.

B. Les États-Unis d'Amérique

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

143. 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 Cour FISA 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.

144. 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.

145. 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 Cour FISA.

146. 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 nº 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

I. QUESTION PRÉLIMINAIRE : LA DATE DE L'APPRÉCIATION

147. Devant la chambre, la requérante avait formulé un grief portant sur la compatibilité avec la Convention de la législation suédoise pertinente telle qu'appliquée pendant trois périodes distinctes (paragraphe 82 de l'arrêt de la chambre). La chambre a décidé de faire porter son contrôle sur la législation suédoise telle qu'en vigueur au moment où elle a examiné l'affaire (paragraphes 96-98 de l'arrêt de la chambre).

148. Devant la Grande Chambre, la requérante n'a pas réitéré sa demande concernant les trois périodes mais s'est appuyée notamment, dans ses observations, sur les évolutions intervenues en 2018 et 2019 après l'examen de l'affaire par la chambre.

149. Le Gouvernement argue que, eu égard à la jurisprudence de la Cour selon laquelle « le contenu et la portée de l'« affaire » renvoyée devant la Grande Chambre sont (...) délimités par la décision de la chambre quant à la recevabilité », le contrôle de la Grande Chambre ne devrait porter que sur la législation suédoise telle qu'en vigueur au moment de l'examen de la chambre.

150. La Grande Chambre souscrit à l'avis de la chambre selon lequel lorsque, comme en l'espèce, la Cour examine un cadre juridique *in abstracto*, sa tâche ne saurait consister à en apprécier la compatibilité avec la Convention avant et après chaque réforme législative.

151. Partant, le champ temporel de l'examen de la Grande Chambre est limité à la législation et à la pratique suédoises telles qu'en vigueur en mai 2018, au moment de l'examen de l'affaire par la chambre.

II. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION

152. La requérante allègue que la législation et la pratique suédoises pertinentes en matière d'interception en masse de communications, activité qui relève du renseignement d'origine électromagnétique (ROEM), ont porté atteinte à son droit au respect de sa vie privée et de sa correspondance tel que protégé par l'article 8 de la Convention. Le Gouvernement conteste cette thèse.

153. L'article 8 de la Convention est 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, au bien-être 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. »

A. Sur l'exception préliminaire du Gouvernement concernant la qualité de victime de la requérante

1. L'arrêt de la chambre

154. Appliquant les critères énoncés dans les arrêts *Roman Zakharov c. Russie* ([GC], n° 47143/06, CEDH 2015) et *Kennedy c. Royaume-Uni* (n° 26839/05, 18 mai 2010), la chambre a considéré que la législation litigieuse sur le ROEM instaurait un système de surveillance secrète susceptible de toucher tous les utilisateurs et qu'aucun recours interne ne permettait à un demandeur soupçonnant que ses communications avaient été interceptées d'obtenir une décision comportant une motivation détaillée. Dans ces conditions, elle a estimé qu'il y avait lieu d'examiner *in abstracto* la législation pertinente, et elle a conclu que la requérante pouvait se prétendre victime d'une violation de la Convention bien qu'elle ne fût pas en mesure d'alléguer avoir fait l'objet d'une mesure concrète d'interception. Pour les mêmes raisons, elle a conclu que la simple existence de la législation en cause constituait en elle-même une ingérence dans l'exercice par la requérante de ses droits protégés par l'article 8.

2. Thèses des parties devant la Grande Chambre

a) Le Gouvernement

155. Le Gouvernement soutient que la requérante n'appartient pas à « un groupe de personnes ou d'entités visées par la législation » relative au ROEM, branche du renseignement extérieur.

156. Il affirme, par ailleurs, que la législation litigieuse n'affecte pas directement l'ensemble des utilisateurs des services de téléphonie mobile et d'Internet puisqu'elle s'applique uniquement au renseignement extérieur et, partant, à des circonstances extérieures au territoire national.

157. Renvoyant aux six étapes des activités de ROEM telles qu'il les a décrites (paragraphe 29 ci-dessus), il avance qu'il est peu probable que les communications par téléphone et sur Internet de la requérante puissent être concernées par des activités de ROEM, et ce pour les raisons suivantes : la majorité des communications purement nationales ne passeraient pas par les points de transfert des câbles transfrontaliers ; en toute hypothèse, les sélecteurs utilisés pour recueillir les signaux pertinents seraient conçus pour

viser très précisément les phénomènes extérieurs ciblés et ils seraient soumis à l'approbation du tribunal pour le renseignement extérieur ; il serait dès lors peu probable que les communications de la requérante soient retenues à l'issue de l'étape de traitement automatisé décrite ci-dessus ; les données passant par les canaux de transmission sans être sélectionnées disparaîtraient sans qu'il soit possible pour le FRA de les reproduire et de les examiner ; enfin, à supposer même que les données ou communications de la requérante atteignent le troisième stade du processus d'interception en masse, le risque qu'elles soient conservées pour examen aux étapes suivantes serait pratiquement inexistant car les informations obtenues feraient encore ensuite l'objet de nouveaux filtrages opérés par des moyens automatiques et manuels.

158. Le Gouvernement estime qu'il n'y a pas ingérence dans l'exercice des droits protégés par l'article 8 tant qu'une analyse des signaux sélectionnés n'est pas possible.

159. Il soutient également qu'en droit suédois, les personnes qui pensent avoir fait l'objet de mesures d'interception de signaux disposent de recours effectifs, notamment de la possibilité de saisir l'Inspection du renseignement extérieur afin que celle-ci leur fasse savoir si leurs données ont fait l'objet d'une collecte inappropriée. Il avance que l'exigence que le recours permette en outre d'obtenir une décision comportant une « motivation détaillée » n'est pas fondée sur la jurisprudence antérieure et qu'en appliquant un tel critère, la chambre a indument ajouté une contrainte supplémentaire.

160. Sur la base de ces arguments, le Gouvernement allègue que la requérante ne pourrait se prétendre victime d'une violation entraînée par la simple existence de la législation contestée que si elle était à même de montrer qu'en raison de sa situation « personnelle » elle est potentiellement exposée au risque de faire l'objet de mesures de ROEM. Il soutient que tel n'est pas le cas en l'espèce et que, bien au contraire, il est improbable que les communications par téléphone et sur Internet de l'intéressée soient interceptées et retenues après filtrage et, en toute hypothèse, le risque qu'elles puissent être sélectionnées pour un contrôle plus approfondi au-delà du stade du traitement automatique est pratiquement inexistant.

161. Le Gouvernement demande donc à la Grande Chambre de déclarer la requête irrecevable pour défaut de qualité de victime de la requérante ou de constater l'absence d'ingérence dans l'exercice par l'intéressée de ses droits protégés par l'article 8.

162. Il ne soulève en revanche aucune exception d'irrecevabilité en ce qui concerne l'épuisement des voies de recours internes.

b) La requérante

163. La requérante soutient que sont réunies dans la présente affaire les deux conditions permettant de prétendre à la qualité de victime dans le cadre

d’une requête concernant l’existence même d’un régime de surveillance secrète, telles qu’énoncées dans l’arrêt *Roman Zakharov* (précité).

164. Elle argue en particulier que la loi relative au renseignement d’origine électromagnétique autorise l’interception de toute communication traversant la frontière suédoise par câble ou transmise par voie aérienne, et qu’elle concerne donc directement l’ensemble des utilisateurs de tels services de communication. Elle ajoute que, même si seule l’interception des communications relatives à des circonstances extérieures au territoire national est autorisée, pratiquement tous les utilisateurs de services de communication peuvent être amenés à communiquer avec l’étranger, que ce soit délibérément en contactant un destinataire étranger ou involontairement en communiquant par l’intermédiaire d’un serveur situé à l’étranger. Elle précise, par ailleurs, que la loi relative au renseignement d’origine électromagnétique autorise les interceptions à des fins de développement de communications sans lien avec des circonstances extérieures.

165. La requérante soutient enfin qu’aucun recours interne effectif ne permet, ni à elle ni à aucune autre personne pensant avoir fait l’objet d’une mesure d’interception en masse de la part des autorités suédoises, de contester ladite mesure. Dès lors, elle plaide, d’une part, qu’il faut qu’elle puisse faire examiner son affaire par la Cour et, d’autre part, qu’elle peut prétendre que l’existence même du régime litigieux porte atteinte à ses droits protégés par l’article 8.

3. Appréciation de la Cour

166. Comme la Cour l’a observé dans les arrêts *Kennedy* et *Roman Zakharov* (précités), il existe, dans les affaires où sont en cause des mesures de surveillance secrète, des considérations particulières justifiant qu’elle déroge à son approche générale déniant aux particuliers le droit de se plaindre *in abstracto* d’une loi. La principale d’entre elles tient à ce qu’il importe de s’assurer que le caractère secret de pareilles mesures ne conduise pas à ce qu’elles soient en pratique inattaquables et échappent au contrôle des autorités judiciaires nationales et de la Cour (*Roman Zakharov*, précité, § 169).

167. Selon une jurisprudence désormais bien établie, il y a lieu d’appliquer plusieurs critères pour déterminer si un requérant peut se prétendre victime d’une violation de ses droits découlant de la Convention qui aurait été entraînée par la simple existence de mesures de surveillance secrète ou d’une législation permettant de telles mesures. Ces critères ont été formulés comme suit dans l’arrêt *Roman Zakharov* (précité, § 171) :

> « Premièrement, la Cour prendra en considération la portée de la législation autorisant les mesures de surveillance secrète et recherchera pour cela si le requérant peut éventuellement être touché par la législation litigieuse, soit parce qu’il appartient à un groupe de personnes visées par elle, soit parce qu’elle concerne directement

> l'ensemble des usagers des services de communication en instaurant un système dans lequel tout un chacun peut voir intercepter ses communications.
>
> Deuxièmement, la Cour tiendra compte de la disponibilité de recours au niveau national et ajustera le niveau de son contrôle en fonction de l'effectivité de ces recours. (...) [L]orsque l'ordre interne n'offre pas de recours effectif à la personne qui pense avoir fait l'objet d'une surveillance secrète, les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance secrète ne sont pas injustifiés (...). Dans ces circonstances, on est fondé à alléguer que la menace de surveillance restreint par elle-même la liberté de communiquer au moyen des services des postes et télécommunications et constitue donc, pour chaque usager ou usager potentiel, une atteinte directe au droit garanti par l'article 8. Un contrôle accru par la Cour s'avère donc nécessaire, et il se justifie de déroger à la règle selon laquelle les particuliers n'ont pas le droit de se plaindre d'une loi *in abstracto*. En pareil cas, la personne concernée n'a pas besoin d'établir l'existence d'un risque que des mesures de surveillance secrète lui aient été appliquées.
>
> Si en revanche l'ordre interne comporte des recours effectifs, des soupçons généralisés d'abus sont plus difficiles à justifier. Dans ce cas de figure, l'intéressé peut se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant de telles mesures uniquement s'il est à même de montrer qu'en raison de sa situation personnelle il est potentiellement exposé au risque de subir pareilles mesures. »

168. Appliquant ces critères au cas d'espèce, la Cour observe d'abord que, comme le fait valoir le Gouvernement, la requérante n'appartient pas à un groupe de personnes ou d'entités visées par les mesures et la législation suédoises adoptées en matière de ROEM. La requérante n'a d'ailleurs rien allégué de tel.

169. Il convient donc d'examiner le point de savoir si, comme le soutient l'intéressée, la législation litigieuse instaure un système de surveillance secrète susceptible de toucher toute personne qui communique par téléphone ou qui utilise Internet.

170. À cet égard, il est clair que les communications ou données de communication de toute personne physique ou morale se trouvant en Suède peuvent être transmises par des canaux de transmission faisant l'objet d'interceptions et être ainsi soumises, en vertu de la législation contestée, tout au moins aux stades initiaux du traitement automatique opéré par le FRA.

171. Le Gouvernement avance que les activités de ROEM ne concernent que les menaces et les circonstances extérieures et que, par conséquent, le risque que les communications de la requérante soient retenues pour un contrôle plus approfondi au-delà du stade de traitement automatique du processus d'interception en masse est pratiquement inexistant. Cette argumentation est pertinente pour l'appréciation de l'intensité et de la proportionnalité de l'atteinte portée aux droits protégés par l'article 8, compte tenu des garanties que présente le système incriminé d'interception des signaux, mais elle n'est pas déterminante pour ce qui est de la qualité de victime de la requérante au sens de l'article 34 de la Convention. Toute

autre interprétation risquerait de subordonner l'accès au mécanisme de recours prévu par la Convention à la possibilité de prouver que les communications d'une personne présentent un intérêt pour les services en charge du renseignement extérieur –tâche pratiquement irréalisable étant donné le secret inhérent aux activités de renseignement extérieur.

172. Dans ces conditions, la Cour doit tenir compte des voies de recours ouvertes en Suède aux personnes qui pensent avoir fait l'objet de mesures prises en application de la loi relative au renseignement d'origine électromagnétique pour déterminer si, comme le soutient la requérante, le risque d'être soumis à une surveillance peut être jugé constitutif en lui-même d'une restriction de la liberté de communiquer et ainsi, pour chaque utilisateur réel ou potentiel, d'une atteinte directe au droit garanti par l'article 8.

173. À cet égard, la Cour observe qu'en pratique les personnes touchées par des activités d'interception en masse ne reçoivent aucune notification. D'un autre côté, toute personne, quels que soient sa nationalité et son lieu de résidence, peut saisir l'Inspection du renseignement extérieur. Celle-ci doit alors rechercher si les communications de cette personne ont été interceptées dans le cadre d'activités de ROEM et, si tel a été le cas, vérifier si l'interception et le traitement des informations correspondantes ont été effectués dans le respect du droit applicable. Elle peut décider de mettre fin à une opération de ROEM ou ordonner la destruction des renseignements recueillis. Toute personne peut également saisir les médiateurs parlementaires et le chancelier de la Justice dans un certain nombre de circonstances.

174. La requérante allègue toutefois que l'Inspection ne peut donner d'autre information que le fait qu'il y a eu une irrégularité, et qu'elle se prononce par une décision définitive non susceptible de recours dans laquelle elle ne motive pas les conclusions auxquelles elle est parvenue. Aucune autre voie de recours ne permettrait au demandeur d'obtenir des informations supplémentaires sur les circonstances d'une éventuelle interception, sur l'utilisation qui a été faite de ses communications ou des données qui s'y rapportent, ni, le cas échéant, sur la nature de la surveillance illégale.

175. En ce qui concerne la question relative à la qualité de victime de la requérante, la Cour observe, sans préjudice des conclusions qui seront tirées relativement aux exigences matérielles des articles 8 § 2 et 13 dans le cas d'espèce, qu'un certain nombre de restrictions s'appliquent aux recours internes ouverts en Suède aux personnes qui pensent être concernées par des mesures d'interception en masse. Elle considère que, même si ces restrictions doivent être considérées comme inévitables ou justifiées, le résultat pratique en est que les recours existants ne sont pas de nature à suffisamment dissiper les craintes de la population quant au risque d'une surveillance secrète.

176. Il s'ensuit qu'il n'est pas nécessaire de déterminer si, en raison de sa situation personnelle, la requérante est potentiellement exposée au risque de voir ses communications ou les données qui s'y rapportent interceptées et analysées.

177. Au vu de ce qui précède, la Cour estime qu'il y a lieu d'examiner *in abstracto* la législation pertinente. Elle rejette donc l'exception du Gouvernement selon laquelle la requérante ne pourrait se prétendre victime d'une violation des droits protégés par la Convention du simple fait de l'existence de la législation et des mesures d'interception en masse adoptées en Suède.

B. Sur le fond

1. L'arrêt de la chambre

178. La chambre a jugé que le système de surveillance en question avait sans conteste une base en droit interne et qu'il était justifié par l'intérêt de la sécurité nationale. Elle a considéré que, compte tenu des menaces que constituent aujourd'hui le terrorisme international et les formes graves de criminalité transfrontière, ainsi que du perfectionnement croissant des technologies de communication, la Suède jouissait d'une grande latitude (une « ample marge d'appréciation ») pour décider d'instaurer un tel système d'interception en masse. Elle a toutefois estimé que cette latitude était plus restreinte en ce qui concernait la mise en œuvre concrète de ce système d'interception et qu'il fallait à cet égard vérifier l'existence de garanties adéquates et effectives contre les abus. Elle a ainsi recherché la présence des garanties minimales contre les abus de pouvoir, telles qu'énoncées dans sa jurisprudence et, en particulier, dans l'arrêt *Roman Zakharov* (précité ; voir les paragraphes 99-115 de l'arrêt de la chambre).

179. Dans l'ensemble, si elle a relevé des possibilités d'amélioration dans certains domaines – notamment l'encadrement de la communication à d'autres États ou à des organisations internationales de données à caractère personnel et la pratique selon laquelle la motivation des décisions prises à l'issue de l'examen des plaintes individuelles n'est pas rendue publique (paragraphes 150, 173 et 177 de l'arrêt de la chambre) – la chambre a estimé que le système ne révélait aucune carence significative dans sa structure et son fonctionnement. Dans ce contexte, elle a observé que le cadre réglementaire avait été révisé à plusieurs reprises pour mieux protéger la vie privée et qu'il avait évolué de telle manière qu'il minimisait le risque d'atteinte à la vie privée, ce qui compensait le manque d'ouverture du système (paragraphes 180 et 181 de l'arrêt de la chambre).

180. La chambre a constaté, plus précisément, que la portée de l'interception et le traitement des données interceptées étaient clairement définis par la loi, que la durée des mesures était clairement encadrée (les autorisations étant valables pour une durée maximale de six mois et leur

renouvellement supposant un réexamen), que la procédure d'autorisation était détaillée et confiée à un organe judiciaire, le tribunal pour le renseignement extérieur, que la supervision et le contrôle du système étaient assurés par plusieurs organes indépendants, notamment l'Inspection du renseignement extérieur et l'autorité de protection des données, et que l'Inspection, les médiateurs parlementaires et le chancelier de la Justice étaient tenus d'examiner les plaintes individuelles dont ils étaient saisis par des personnes craignant que leurs communications aient été interceptées (paragraphes 116-147 et 153-178 de l'arrêt de la chambre).

181. La chambre a donc conclu que le système suédois de ROEM offrait des garanties adéquates et suffisantes contre l'arbitraire et le risque d'abus. Elle a jugé que la législation pertinente répondait à l'exigence relative à la « qualité de la loi » et que l'ingérence constatée pouvait être considérée comme « nécessaire dans une société démocratique ». Elle a enfin estimé que la structure et le fonctionnement du système étaient proportionnés au but visé. Elle a toutefois souligné que sa conclusion résultait d'un examen *in abstracto* et n'empêcherait pas d'examiner la responsabilité de l'État au regard de la Convention dans le cas où, par exemple, la requérante aurait connaissance d'une interception dont elle aurait effectivement fait l'objet (paragraphes 179-181 de l'arrêt de la chambre).

2. Thèses des parties

a) La requérante

i. La position de la requérante quant au critère à appliquer

182. La requérante soutient que les régimes d'interception en masse sont intrinsèquement incompatibles avec la Convention. Elle souligne que dans les arrêts *Klass et autres c. Allemagne* (6 septembre 1978, § 51, série A n° 28) et *Association « 21 Décembre 1989 » et autres c. Roumanie* (n^{os} 33810/07 et 18817/08, §§ 174-175, 24 mai 2011), la Cour a jugé problématique la surveillance « exploratoire » ou « générale ». Elle allègue qu'en matière d'interception non ciblée, les seuls régimes que la Cour a jugés compatibles avec la Convention avaient une portée beaucoup plus restreinte que celle du régime suédois. Elle ajoute que le FRA peut avoir accès à quasiment toutes les communications par câble qui traversent la frontière suédoise et que, dès lors, la quantité de données intimes, privées ou protégées par le secret professionnel qui peuvent être examinées dans le cadre du système suédois de ROEM est beaucoup plus importante. Elle soutient que seuls des régimes d'interception ciblée ou des régimes d'interception non ciblée à plus petite échelle peuvent relever de la marge d'appréciation des États. Selon elle, toute autre approche risquerait d'aboutir à une jurisprudence incohérente, compte tenu de l'interprétation adoptée par la Cour relativement à d'autres questions formulées sur le terrain de la Convention, notamment celle de la conservation générale des

empreintes digitales et des profils ADN, examinée dans l'arrêt *S. et Marper c. Royaume-Uni* ([GC], nos 30562/04 et 30566/04, § 115, CEDH 2008).

183. La requérante soutient que si la Cour considère que les activités d'interception en masse peuvent être justifiées au regard de la Convention, il est impératif que de solides garanties minimales soient établies. Elle avance que les éléments exposés dans l'arrêt *Roman Zakharov* (précité, § 238) pourraient servir de cadre initial mais que la surveillance non ciblée comporte des risques élevés d'atteinte à la vie privée et qu'il faut donc en la matière adapter ces critères.

184. Elle estime en particulier que les principaux éléments du régime d'interception devraient être définis de manière suffisamment détaillée dans une loi : cela garantirait, selon elle, que ce sont bien les représentants du peuple qui fixent l'équilibre entre les intérêts concurrents.

185. Pour ce qui est de l'autorisation préalable, la requérante admet que l'organe qui est compétent pour l'accorder en Suède est de nature judiciaire, mais elle invite la Cour à aller un peu plus loin dans sa jurisprudence en exigeant que l'autorisation préalable ait toujours un caractère judiciaire.

186. De surcroît, elle avance que l'organe chargé d'accorder l'autorisation devrait être en mesure de vérifier que les personnes ciblées à titre individuel ou collectif par des activités d'interception ne fassent l'objet d'une telle surveillance que sur le fondement d'un soupçon raisonnable. Elle trouve peu convaincant l'écart opéré par la Cour dans la présente affaire et dans l'affaire *Big Brother Watch et autres c. Royaume-Uni* (nos 58170/13 et 2 autres, 13 septembre 2018) par rapport à ce critère selon elle bien établi. Elle estime que l'utilisation de sélecteurs personnalisés pour isoler et collecter des données sur un individu précis dans le contexte de l'interception en masse devrait être soumise au même seuil que celui qui s'applique aux interceptions ciblées, et que si tel n'était pas le cas, ces sélecteurs pourraient être employés pour cibler des individus en contournant les règles applicables à la surveillance individuelle.

187. La requérante ajoute qu'en l'absence de cibles prédéfinies, l'organe chargé d'accorder l'autorisation devrait être en mesure de vérifier que des données à caractère personnel ne sont utilisées dans les sélecteurs que dans la mesure où elles sont importantes pour un objectif de renseignement extérieur étroitement défini. Elle expose à cet égard que l'utilisation de sélecteurs se rapportant à un individu en particulier expose celui-ci à des risques spécifiques d'atteinte à la vie privée, notamment en ce qui concerne le caractère intime de certaines questions et opinions.

188. Par ailleurs, elle soutient que l'organe chargé d'accorder l'autorisation devrait être informé de la manière dont les données seront analysées et utilisées (par exemple, si les analystes entendent procéder à l'exploration de données par schéma ou par sujet, et si des profils d'individus seront établis).

189. Pour ce qui est de la supervision au moment de la mise en œuvre des activités de surveillance et après leur achèvement, la requérante admet que les organes de supervision suédois sont suffisamment indépendants de l'exécutif.

190. Elle argue toutefois que l'organe de supervision doit être investi de pouvoirs suffisants pour adopter des décisions juridiquement contraignantes, par lesquelles il puisse notamment faire cesser et réparer toute irrégularité et engager la responsabilité de ses auteurs, qu'il doit avoir accès aux documents classifiés, et que ses activités doivent être soumises à un droit de regard du public. Elle estime que les pouvoirs de supervision devraient concerner à la fois les données de contenu et les données de communication et qu'ils devraient être exercés au stade où les communications recueillies sont soumises à une analyse informatique automatisée, au stade où des analystes en chair et en os interviennent et au stade où les informations sont communiquées à des autorités nationales, à des gouvernements étrangers ou à des organisations internationales. Elle ajoute que la conservation des données à chaque stade devrait également faire l'objet d'une supervision.

191. Elle considère qu'il faut en outre que les personnes concernées disposent de recours effectifs, qui peuvent revêtir trois formes : la notification de la surveillance à la personne concernée après que la surveillance a cessé, la possibilité de demander des informations sur la surveillance, ou l'existence d'un organe qui puisse examiner les plaintes d'un individu sans que celui-ci soit tenu de produire des éléments de preuve.

192. Pour ce qui est de la communication des éléments interceptés à des acteurs étrangers, la requérante argue que les États contractants ne jouissent pas d'une latitude illimitée et qu'ainsi, ils ne peuvent pas sous-traiter des opérations de traitement et d'analyse de données de manière à contourner leur responsabilité au regard de la Convention. Elle soutient que les garanties minimales doivent comporter des dispositions juridiques accessibles, posant des conditions qui encadrent clairement le partage de données, et notamment l'obligation de prendre des mesures raisonnables pour s'assurer que la partie destinataire protège les données avec, d'une part, des garanties similaires à celles applicables dans l'État qui les communique et, d'autre part, des mécanismes de supervision et de recours suffisants.

ii. L'analyse par la requérante du régime suédois contesté

193. Appliquant ces critères au régime suédois contesté, la requérante admet que le champ d'application général des pouvoirs du FRA est suffisamment délimité, à l'exception de la grande latitude dont cet organisme jouit en ce qui concerne ses activités de développement. Elle exprime toutefois des préoccupations quant au fait que la Sûreté et la direction des opérations nationales de l'autorité de police (« la NOA ») sont

autorisées, depuis le 1er janvier 2013, à adopter des directives d'attribution de tâches de ROEM, et que, depuis le 1er mars 2018, la Sûreté peut se voir accorder un accès direct aux bases de données du FRA contenant des éléments analysés. Elle plaide que le risque d'une utilisation du ROEM hors du champ des activités de renseignement extérieur doit être suffisamment encadré par des dispositions juridiques claires, ainsi que par une supervision effective.

194. La requérante indique également que si la loi suédoise sur le renseignement d'origine électromagnétique exige que les mandats d'interception soient assortis d'une date d'expiration précise, il n'est pas obligatoire d'annuler un mandat dès lors que la collecte de communications qu'il autorise cesse d'être nécessaire.

195. Elle soutient par ailleurs que la portée du contrôle judiciaire exercé par l'organe chargé d'accorder les autorisations en Suède – le tribunal pour le renseignement extérieur – est trop limitée pour être effective. Elle allègue, en particulier, que l'existence d'un soupçon raisonnable à l'égard de la personne ciblée n'est pas vérifiée et que le critère de l'« importance exceptionnelle » justifiant l'utilisation de sélecteurs se rapportant directement à un individu ne s'applique qu'aux sélecteurs employés dans le cadre de la collecte automatisée de données, et non à l'étape où les données collectées font l'objet d'une recherche plus approfondie. Elle ajoute que le tribunal pour le renseignement extérieur n'est pas tenu de contrôler l'utilisation qu'il est prévu de faire des données recueillies, et qu'il n'est d'ailleurs pas précisé dans les demandes de mandat comment les données seront analysées, par exemple si elles feront l'objet d'une exploration de données par sujet ou si des profils d'individus seront établis.

196. Pour ce qui est de la conservation, de la consultation, de l'examen, de l'utilisation et de la destruction des données interceptées, la requérante avance que le système suédois comporte deux failles majeures : d'une part, l'absence d'obligation pour le FRA de tenir des archives détaillées concernant les interceptions, l'utilisation et la communication des données, ce que l'autorité suédoise de protection des données aurait critiqué à plusieurs reprises, et d'autre part, l'absence de règles spécifiquement adaptées à l'interception en masse, distinctes des règles générales sur le traitement des données. Elle se déclare par ailleurs préoccupée par le fait que, depuis le 1er mars 2018, la Sûreté peut se voir accorder un accès direct aux bases de données du FRA contenant des éléments analysés.

197. La requérante allègue également que les personnes morales ne bénéficient pas d'une protection adéquate car la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA ne s'applique qu'aux éléments interceptés contenant des données à caractère personnel. Il en résulte, selon elle, que les éléments qui ne contiennent pas de données à caractère personnel peuvent être conservés indéfiniment et utilisés dans un but incompatible avec l'objectif initial de la collecte.

198. La requérante critique aussi plusieurs caractéristiques du système de supervision existant. Elle indique, premièrement, que même si, lorsqu'elle estime qu'une opération de ROEM est incompatible avec le mandat délivré par le tribunal pour le renseignement extérieur, l'Inspection peut décider que l'opération en question doit cesser ou que les renseignements collectés doivent être détruits, elle n'a pas le pouvoir de rendre des décisions contraignantes lorsqu'elle juge le mandat illégal, ni le pouvoir d'accorder une réparation ou d'engager la responsabilité des auteurs d'irrégularités. Elle allègue, deuxièmement, que ni l'autorité de protection des données ni le chancelier de la Justice ni les médiateurs ne peuvent rendre des décisions juridiquement contraignantes. Elle précise que l'autorité de protection des données peut seulement saisir le tribunal administratif de Stockholm pour obtenir la destruction des données ayant fait l'objet d'un traitement illégal, et qu'aucune des plaintes qui ont été adressées au chancelier de la Justice ou aux médiateurs quant aux activités du FRA n'a abouti. Elle affirme que ces organes ne sont pas spécialisés dans les activités du FRA et qu'ils n'ont ni les connaissances ni la capacité nécessaires pour les superviser de manière effective.

199. Sur les recours disponibles dans le régime suédois contesté, la requérante émet les observations suivantes.

Premièrement, la notification prévue à l'article 11 a) de la loi relative au renseignement d'origine électromagnétique ne concernerait que les personnes physiques, et non les personnes morales ; en outre, l'obligation de notifier pourrait être levée dans les cas où le secret l'exige, ce qui se produirait constamment dans la pratique. Ce recours serait donc « théorique et illusoire ». La possibilité de demander au FRA de faire savoir à un individu si des données à caractère personnel le concernant ont fait l'objet d'un traitement serait aussi soumise à la règle du secret ; et le tribunal administratif pourrait certes être saisi subséquemment, mais il n'aurait pas accès aux documents secrets et ne serait donc pas en mesure de contrôler l'appréciation faite par le FRA de la nécessité d'appliquer les restrictions liées au secret. De plus, ce recours ne serait pas non plus ouvert aux personnes morales, et la requérante ne pourrait donc pas l'exercer.

Deuxièmement, la requérante indique qu'au Royaume-Uni, un organe judiciaire indépendant, l'IPT, a compétence pour connaître des plaintes individuelles d'interception illégale sans qu'il soit nécessaire pour les personnes concernées de prouver qu'elles ont fait l'objet d'une surveillance. Elle précise que cet organe a accès aux documents secrets, peut rendre des décisions juridiquement contraignantes – qui sont publiées – et accorder une réparation. Elle soutient qu'un tel système n'existe pas en Suède.

Troisièmement, pour ce qui est de la possibilité en droit suédois de demander à l'Inspection de rechercher si les communications d'une personne ont été interceptées, la requérante observe que l'Inspection n'informe pas la personne concernée de ses conclusions et n'envoie que des

réponses standardisées indiquant qu'aucune surveillance illégale n'a été menée. Elle répète que l'Inspection n'a pas le pouvoir de contrôler le respect de la loi et de la Constitution, ni d'accorder une réparation.

Quatrièmement, la requérante soutient que la possibilité d'introduire une demande d'indemnisation auprès du chancelier de la Justice ne constitue pas un recours effectif. Elle avance à cet égard les arguments suivants : i) ce serait à la personne concernée qu'il incombe de prouver qu'il y a eu surveillance illégale, ii) l'octroi d'une indemnisation non accompagné de la suppression des données traitées illégalement ne pourrait être considéré comme un redressement effectif, iii) le chancelier, qui aurait toute latitude pour déterminer quelles plaintes examiner, aurait rejeté à ce jour toutes les plaintes concernant les activités du FRA, et iv) le Gouvernement n'aurait pas démontré l'effectivité de ce recours, faute d'avoir indiqué les mesures que le chancelier est tenu de prendre lorsqu'il reçoit un rapport de l'Inspection l'informant d'activités du FRA susceptibles de donner lieu à des demandes d'indemnisation : or, pour donner à un individu la possibilité de présenter une demande d'indemnisation, le chancelier devrait inévitablement l'informer du comportement illégal du FRA, démarche à laquelle le secret pourrait faire obstacle.

Cinquièmement, la requérante affirme qu'en l'absence de notification ou d'accès aux documents, il est pratiquement impossible pour le demandeur, dans une action en réparation intentée au civil, de s'acquitter de la charge de la preuve.

Sixièmement, la requérante plaide que les médiateurs ne peuvent accorder aucune forme de réparation et que le Gouvernement n'a produit aucun exemple de nature à démontrer l'effectivité de ce recours.

Septièmement, elle argue que la procédure par laquelle le FRA peut corriger ou détruire des données à caractère personnel ayant fait l'objet d'un traitement illégal suppose que la personne sache que des données la concernant ont été traitées, et que le secret la rend par conséquent ineffective. Elle souligne également que le tribunal administratif n'a jamais reçu de la part de l'autorité de protection des données de demande de destruction de données ayant fait l'objet d'un traitement illégal.

Enfin, la possibilité de signaler une affaire à des fins de poursuites supposerait également que la personne concernée ait connaissance des irrégularités pertinentes, et, de ce fait, serait elle aussi ineffective.

200. Sur la question de la transmission des données interceptées à des tiers étrangers, la requérante soutient que le régime juridique et la pratique en vigueur en Suède sont entachés de défaillances manifestes. Elle observe que les limitations légales apportées à cette transmission ne consistent qu'en une obligation vague et générale d'agir dans l'intérêt national, mais qu'il n'existe aucune exigence imposant de prendre en compte le préjudice susceptible d'être causé à la personne concernée ou d'obliger le destinataire

à protéger les données par des garanties similaires à celles applicables en Suède.

201. La requérante exprime son désaccord avec la conclusion de la chambre selon laquelle les carences susmentionnées seraient contrebalancées par les mécanismes de supervision que comprend le système suédois. Elle soutient que cette supervision est inadéquate et que, en tout état de cause, elle ne s'applique pas à la communication à des tiers étrangers de données interceptées. Elle indique que le FRA est seulement tenu d'informer l'Inspection des principes régissant sa coopération avec des tiers étrangers, de préciser les pays et les organisations internationales auxquels les données sont communiquées et de fournir des informations générales concernant les opérations. Elle avance que même si l'Inspection contrôle la conformité des activités du FRA avec les exigences légales existantes, la loi accorde au FRA une latitude excessive dans ce domaine, de sorte que même le contrôle le plus étroit de l'Inspection ne pourrait guère offrir de garanties contre les abus. Elle conclut que les modalités exposées ci-dessus permettent de sous-traiter tout simplement des activités qui seraient normalement illicites, sans respecter les limites appropriées protégeant les droits fondamentaux, et que dans ces conditions, elles ne peuvent constituer une pratique compatible avec la Convention.

b) Le Gouvernement

202. Le Gouvernement expose que les activités de ROEM visent à obtenir des informations et à repérer des phénomènes présentant un intérêt pour le renseignement extérieur. Il souligne que celui-ci est d'une importance capitale pour la sécurité nationale de la Suède et qu'il est également important au regard de l'obligation positive que la Convention fait peser sur l'État de protéger la vie et la sécurité du public.

203. Le Gouvernement fait observer que, à l'exception de la présente affaire et de l'affaire *Big Brother Watch*, la jurisprudence dans laquelle la Cour a établi des garanties minimales en matière de mesures de surveillance secrète concerne des enquêtes pénales. Il en déduit que certaines de ces garanties minimales supposent que les mesures en cause s'appliquent à un individu ou à un lieu précis. Il argue que la situation est très différente dans le contexte des activités de ROEM puisque celles-ci ne peuvent être utilisées pour enquêter sur des infractions pénales – l'une des missions du tribunal pour le renseignement extérieur serait d'ailleurs de s'assurer que tel n'est pas le cas. Il ajoute que si les activités de ROEM, qui relèvent du renseignement extérieur, peuvent dans bien des cas cibler les communications d'individus déterminés, ceux-ci ne présentent le plus souvent pas d'intérêt en tant que tels, mais ne sont que des vecteurs des informations recherchées.

204. Dans ce contexte, le Gouvernement soutient que les exigences pertinentes doivent être adaptées, notamment par la reformulation de certains

des critères énoncés dans la jurisprudence de la Cour. Ainsi, il conviendrait de remplacer les critères de « la nature des infractions » et des « catégories de personnes ciblées » par celui des « circonstances dans lesquelles les mesures peuvent être utilisées ». Il faudrait également tenir compte du fait que les menaces qui pèsent sur la sécurité nationale sont par nature variables et difficiles à définir à l'avance.

205. Le Gouvernement se déclare en profond désaccord avec la requérante lorsqu'elle soutient, en s'appuyant sur les arrêts *Roman Zakharov* (précité) et *Szabó et Vissy c. Hongrie* (nº 37138/14, 12 janvier 2016), que l'existence d'un soupçon raisonnable devrait être exigée à tout le moins lorsque sont utilisés des sélecteurs se rapportant à une personne donnée. Il plaide qu'aucune obligation de ce type ne peut être tirée de la jurisprudence précitée, et il souscrit au raisonnement de la chambre qui, au paragraphe 317 de l'arrêt *Big Brother Watch*, a estimé que les exigences de « soupçon raisonnable » et de « notification subséquente » étaient incompatibles avec un régime d'interception en masse.

206. Le Gouvernement soutient par ailleurs que les interceptions en masse sont encadrées en Suède par un régime juridique complet fondé sur des dispositions publiées, et que ce régime offre d'importantes garanties, notamment un mécanisme de supervision indépendant des activités de surveillance qui s'applique à la fois aux données de communication et au contenu des communications. Il ajoute que la législation délimite clairement l'étendue des activités de surveillance, le pouvoir conféré aux autorités compétentes dans ce domaine, et la manière de l'exercer.

207. Le Gouvernement affirme que les activités de développement menées par le FRA sont strictement réglementées et qu'elles sont soumises à toutes les exigences matérielles et procédurales applicables aux activités de ROEM en général. Il précise que ce sont le flux du trafic et les systèmes par lesquels les informations sont transmises qui présentent un intérêt pour ces activités, lesquelles seraient essentielles pour permettre au FRA d'adapter ses outils, ses systèmes et ses méthodes aux progrès techniques et à un environnement électromagnétique en constante évolution. Il soutient que limiter les activités de développement aux huit buts dans lesquels des activités de ROEM peuvent être menées serait bien trop restrictif pour que le FRA puisse conserver ses capacités.

208. Le Gouvernement rappelle par ailleurs que les mesures de ROEM font l'objet d'une procédure d'autorisation préalable menée devant le tribunal pour le renseignement extérieur, dont le président et les autres membres sont des juges permanents nommés par le gouvernement pour un mandat de quatre ans. Il reconnaît qu'en cas d'urgence exceptionnelle le FRA peut lui-même accorder une autorisation de mener des activités de ROEM, mais il précise que le tribunal pour le renseignement extérieur doit alors en être averti immédiatement, et peut modifier ou retirer l'autorisation, auquel cas les données collectées doivent être détruites. Il ajoute que si

l'autorisation accordée par le FRA, et non par le tribunal, prévoit un accès à certains canaux de transmission, cet accès ne peut être matériellement ouvert que par l'Inspection suédoise du renseignement extérieur, qui a ainsi la possibilité d'évaluer les aspects juridiques pertinents.

209. Le Gouvernement explique que le tribunal pour le renseignement extérieur tient des audiences publiques sauf lorsque le secret exige une audience à huis clos. Il affirme que cette limitation de la transparence est justifiée et qu'elle est compensée par des garanties, telles que la présence aux audiences à huis clos d'un représentant chargé de la protection de la vie privée. Il précise que ce représentant protège l'intérêt public, a accès à l'ensemble du dossier de l'affaire et peut faire des déclarations, et qu'il doit être ou avoir été juge permanent ou membre de l'association du barreau suédois.

210. Le Gouvernement souligne que le FRA a l'obligation de soumettre une demande d'autorisation pour chaque mission et qu'il doit y indiquer la teneur de la mission, les canaux de transmission auxquels il souhaite accéder et les sélecteurs ou au moins les catégories de sélecteurs qui seront utilisés. Il précise que le tribunal examine non seulement la légalité formelle mais aussi la proportionnalité de l'ingérence prévue. Il ajoute que l'autorisation doit préciser tous les paramètres de la mission, y compris les conditions nécessaires à la limitation de l'ingérence.

211. Pour ce qui est des garanties relatives à la durée de l'interception, le Gouvernement expose que le droit suédois impose une limite de six mois, susceptible de prorogation après examen complet par le tribunal pour le renseignement extérieur. Il précise que lorsqu'une directive d'attribution de tâches est annulée ou arrive à expiration, que l'interception n'a pas respecté l'autorisation sur laquelle elle était fondée ou qu'elle n'est plus nécessaire, il est mis fin à la mesure.

212. Selon le Gouvernement, le système comprend aussi des garanties adéquates relativement aux procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation et la destruction des données interceptées : la limitation du traitement à ce qui est adéquat et pertinent au regard de sa finalité, l'habilitation des agents, l'obligation de confidentialité à laquelle ils sont soumis et les sanctions qu'ils encourent en cas de mauvaise gestion des données. Le Gouvernement précise que les données obtenues doivent être immédiatement détruites dans un certain nombre de circonstances, notamment lorsqu'elles concernent des sources médiatiques protégées en vertu de la Constitution ou des informations relevant de la confidentialité des échanges entre les suspects d'infractions pénales et leur avocat. Il ajoute que s'il apparaît que les communications interceptées étaient purement intérieures, les données correspondantes doivent de même être détruites.

213. En ce qui concerne les conditions dans lesquelles les données interceptées peuvent être communiquées à d'autres parties, le

Gouvernement expose que le FRA a l'obligation juridique d'informer les autorités suédoises concernées et qu'il doit veiller à ce que les données à caractère personnel ne soient communiquées que si elles sont pertinentes au regard des finalités pour lesquelles il peut être mené des activités de renseignement extérieur. Il ajoute que le respect de cette exigence est contrôlé par l'Inspection du renseignement extérieur.

214. Le Gouvernement souligne que même si le FRA est autorisé par la loi à donner aux services gouvernementaux, aux forces armées, à la Sûreté et à trois autres organes un accès direct aux rapports de renseignement qu'il a établis, il n'a pris à ce jour aucune décision en ce sens. Il précise, en outre, que l'article 15 de la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA permet certes à la Sûreté et aux forces armées, depuis le 1er mars 2018, de se voir accorder un accès direct, afin d'opérer des évaluations stratégiques des menaces terroristes, à des données qui constituent le résultat d'analyses réalisées dans une compilation de données établie à cette fin, mais que cela ne change rien à l'interdiction d'utiliser pour enquêter sur des infractions pénales des informations issues des activités de ROEM menées aux fins du renseignement extérieur.

215. Enfin, en ce qui concerne la communication à d'autres États ou à des organisations internationales de données à caractère personnel, le Gouvernement conteste la conclusion de la chambre selon laquelle le régime juridique applicable présente des lacunes (paragraphe 150 de l'arrêt de la chambre). Il argue notamment que le FRA doit aviser le ministère de la Défense avant d'établir et d'entretenir une coopération avec d'autres États ou avec des organisations internationales, et l'informer des questions importantes qui se posent dans le cadre de cette coopération. Il ajoute que le FRA doit faire savoir à l'Inspection suédoise du renseignement extérieur les principes qui s'appliquent à la coopération qu'il entretient avec des partenaires extérieurs et préciser les pays et les organisations avec lesquels il coopère, et qu'une fois la coopération établie, le FRA doit informer l'Inspection de son étendue et, lorsque cela se justifie, des résultats obtenus, de l'expérience acquise et de la poursuite du partenariat.

216. Le Gouvernement souligne également que dans le cadre de la coopération internationale les données sont exclusivement communiquées à des parties menant elles-mêmes des activités de renseignement extérieur, ce qui signifie selon lui qu'il est dans l'intérêt du destinataire des données de les protéger. Il plaide que la confiance entre les parties repose sur leur intérêt mutuel à préserver la sécurité des données. Il ajoute que les directives générales du FRA disposent que toute coopération internationale est subordonnée au respect par l'État destinataire de la législation suédoise. Il précise que les partenaires étrangers reçoivent des informations et une formation sur le contenu pertinent de la législation suédoise. Il affirme que, l'Inspection étant expressément compétente pour contrôler les activités du FRA en matière de coopération internationale, aucune modification

apportée aux directives internes de ce dernier ne pourrait passer inaperçue. Il en conclut que des garanties claires empêchent de contourner le droit suédois.

217. Le Gouvernement soutient par ailleurs que le système suédois de supervision de l'application des mesures de ROEM offre d'importantes garanties. Il argue que l'Inspection du renseignement extérieur est indépendante, qu'elle a accès à tous les documents pertinents, qu'elle examine les sélecteurs employés et qu'elle peut décider de mettre fin à une opération ou ordonner la destruction des données recueillies si la collecte n'a pas respecté l'autorisation sur laquelle elle était fondée. Il ajoute que l'Inspection s'assure aussi que le FRA n'a accès aux canaux de transmission que dans la mesure permise par une autorisation. Il précise qu'elle établit des rapports annuels publics et que ses activités sont soumises au contrôle de la Direction nationale du contrôle de la gestion publique et à la supervision des médiateurs parlementaires et du chancelier de la Justice. En ce qui concerne les données à caractère personnel, il expose que l'autorité suédoise de protection des données exerce des fonctions générales de contrôle. Selon lui, ce type de supervision par des organes non judiciaires indépendants est adéquat et conforme à la jurisprudence de la Cour.

218. Le Gouvernement indique qu'entre 2009 et 2018, l'Inspection a réalisé 113 inspections du FRA, qui ont abouti à la remise de dix-huit avis. Il précise qu'au cours d'au moins dix-sept de ces inspections, elle a vérifié, notamment, si le FRA utilisait les sélecteurs d'une manière compatible avec les autorisations qui lui avaient été délivrées par le tribunal pour le renseignement extérieur, et que dans le cadre d'au moins neuf de ces inspections, elle a examiné des questions relatives à la destruction des données. Il ajoute qu'un certain nombre d'inspections concernaient également la gestion par le FRA de données à caractère personnel. Il fait observer que l'ensemble de ces inspections n'a donné lieu qu'à un faible nombre d'observations et d'avis. Il expose qu'au cours de la même période, l'Inspection a mené 141 contrôles à la demande d'une personne qui souhaitait savoir si ses communications avaient fait l'objet de mesures de ROEM illégales, et qu'aucun d'entre eux n'a révélé d'interception irrégulière. Il indique enfin que plusieurs inspections thématiques des activités du FRA ont aussi été menées, notamment sur le respect des limites posées dans les autorisations.

219. Le Gouvernement soutient par ailleurs qu'il existe plusieurs moyens permettant à un individu de faire vérifier la légalité de mesures prises dans le cadre de la mise en œuvre du système de ROEM. Il expose ainsi que toute personne peut saisir l'Inspection, et être ainsi informée, éventuellement, de la commission d'une irrégularité, demander au FRA si des données à caractère personnel la concernant ont été traitées, saisir les médiateurs parlementaires, le chancelier de la Justice et l'autorité de protection des données, introduire une action en réparation, ou encore

signaler un cas à des fins de poursuites. Il ajoute que certains de ces recours ne sont pas subordonnés à une notification préalable de la mesure à l'individu concerné et que, s'il est impossible de procéder à une notification systématique, il est important de relever que lorsque le FRA a employé des sélecteurs visant directement une personne physique déterminée, il est tenu de l'en aviser, sauf lorsque le secret est requis.

220. Le Gouvernement explique enfin que le cadre juridique suédois régissant l'interception en masse ne distingue pas les données de contenu des données de communication, et que toutes les garanties s'appliquent aux unes comme aux autres. Il expose qu'en pratique l'utilisation de données de communication pour détecter des menaces inconnues nécessite de rassembler divers éléments de ces données pour obtenir un tout à partir duquel on pourra tirer des conclusions, et qu'il en découle, d'une part, que les sélecteurs utilisés pour l'interception des données de communication sont moins spécifiques que ceux utilisés pour le contenu des communications et, d'autre part, que les données en question doivent être accessibles par un analyste pour examen pendant un certain temps. Il assure qu'il n'existe pas d'autres différences.

221. En conclusion, le Gouvernement soutient que le régime contesté de ROEM mis en œuvre aux fins du renseignement extérieur ne révèle aucune carence significative dans sa structure ni dans son fonctionnement. Il allègue que le risque d'atteinte à la vie privée est réduit et que des garanties suffisantes contre l'arbitraire sont en place. Il considère que le régime dans son ensemble est licite et proportionné au but légitime de protection de la sécurité nationale.

3. Les tiers intervenants

a) Le gouvernement de la République d'Estonie

222. Le gouvernement estonien considère que les critères d'appréciation de la compatibilité avec la Convention d'un régime de surveillance secrète, tels qu'énoncés dans la jurisprudence de la Cour, doivent être adaptés pour refléter la nature spécifique de l'interception en masse de communications dans le cadre du renseignement extérieur. Il argue que les différences entre cette activité et la surveillance opérée dans le contexte d'une enquête pénale doivent être prises en compte : le renseignement extérieur viserait à détecter des menaces pour la sécurité nationale et sa portée serait donc plus large. Il plaide également que le renseignement extérieur est une activité à long terme, qui exige un degré plus élevé de secret pendant une période plus longue.

223. Pour ces raisons, et compte tenu des critères d'appréciation appliqués dans l'arrêt *Roman Zakharov* (précité, § 231), le gouvernement estonien souscrit à la conclusion de la chambre selon laquelle les critères de la « nature des infractions » et du « soupçon raisonnable » ne sont pas

appropriés, et il estime qu'au lieu des « catégories de personnes », le droit interne devrait indiquer les « domaines dans lesquels l'interception en masse de communications transfrontières peut être utilisée pour recueillir des renseignements ». Pour ce qui est de la notification aux personnes concernées, il plaide qu'aucune obligation ne devrait être imposée en ce sens, eu égard à l'importance du secret dans les activités de renseignement extérieur.

b) Le gouvernement de la République française

224. Le gouvernement français souligne l'importance des activités d'interception en masse pour la détection de menaces inconnues et plaide que les critères d'appréciation de leur compatibilité avec la Convention, tels qu'énoncés dans la décision *Weber et Saravia c. Allemagne* (n° 54934/00, CEDH 2006-XI) et dans l'arrêt *Roman Zakharov* (précité), sont pertinents dans le cas d'espèce. Il soutient toutefois que, compte tenu de la nature particulière des opérations d'interception en masse, qui diffèrent de la surveillance secrète d'une personne déterminée, aucune exigence de « soupçon raisonnable » ne devrait s'y appliquer.

225. Le gouvernement français est également d'avis que les États jouissent d'une large marge d'appréciation dans la mise en œuvre de régimes d'interception en masse et que l'appréciation du point de savoir s'ils appliquent des garanties contre les abus suffisantes doit toujours se faire *in concreto*, eu égard à la législation pertinente prise dans son ensemble. Il estime que c'est exactement ce qu'a fait la chambre dans la présente affaire, où elle a constaté que, même si quelques améliorations étaient souhaitables, le système suédois dans son ensemble ne comportait pas de lacunes importantes. Il observe toutefois que dans l'arrêt *Big Brother Watch et autres* (précité), la chambre s'est livrée à un examen plus sévère et a conclu, de manière selon lui injustifiée, à la violation des articles 8 et 10 de la Convention. Il se dit en désaccord avec cette dernière approche : il estime, en particulier, qu'un régime d'interception en masse qui ne prévoit pas d'autorisation judiciaire préalable est compatible avec l'article 8 dès lors qu'il comporte un mécanisme de supervision *a posteriori* opérée par un organe indépendant.

226. S'appuyant sur des références à la jurisprudence, il exprime aussi l'avis que l'interception et le traitement de données de communication portent une atteinte moins importante au droit au respect de la vie privée que l'interception et le traitement du contenu des communications, et qu'ils ne devraient donc pas être soumis aux mêmes garanties de protection du droit à la vie privée.

227. Pour ce qui est du partage de renseignements, il souligne l'importance du secret et le fait que les procédures et garanties appliquées peuvent varier d'un État à l'autre. Il expose plusieurs critères applicables en

la matière, en particulier dans le contexte de la réception et de l'utilisation de données interceptées par des partenaires étrangers.

c) Le gouvernement du Royaume des Pays-Bas

228. Le gouvernement néerlandais soutient que l'interception en masse est nécessaire pour repérer des menaces jusqu'alors inconnues pesant sur la sécurité nationale. Il plaide qu'afin de protéger la sécurité nationale, les services de renseignement ont besoin d'outils qui leur permettent de mener des enquêtes promptes et effectives sur des menaces nouvelles et que, pour ce faire, ils doivent disposer de pouvoirs leur permettant de détecter et de prévenir non seulement les activités terroristes (préparation d'attentats, recrutement, propagande, financement), mais aussi les cyberactivités intrusives d'acteurs étatiques ou non étatiques qui visent à saper la démocratie (par exemple en influençant des élections nationales ou en entravant les enquêtes menées par des organisations nationales ou internationales). Il cite l'exemple de la tentative d'interférence (*hacking*) dans l'enquête menée par l'Organisation pour l'interdiction des armes chimiques (sise à La Haye) sur l'utilisation d'armes chimiques en Syrie. Il affirme par ailleurs que des secteurs essentiels, tels que la gestion de l'eau, l'énergie, les télécommunications, les transports, la logistique, les ports et les aéroports, sont de plus en plus dépendants des infrastructures numériques et, de ce fait, de plus en plus vulnérables aux cyberattaques, et que des perturbations dans ces secteurs auraient un impact profond sur la société, bien au-delà du préjudice financier considérable qu'il causerait.

229. Le gouvernement néerlandais expose encore que le développement de nouveaux moyens de communication numérique et l'accroissement exponentiel des données transmises et conservées au niveau mondial sont des facteurs qui rendent la situation plus complexe encore et que, dans bien des cas, la nature et l'origine de la menace sont inconnues et il est donc impossible de cibler les interceptions. Il affirme toutefois que si l'interception en masse n'est pas aussi étroitement paramétrée qu'une interception ciblée, elle n'est jamais totalement dépourvue de cible et elle est au contraire appliquée à des fins spécifiques.

230. Il soutient qu'il n'est pas nécessaire de compléter ou d'actualiser les exigences minimales qui ont déjà été énoncées par la Cour : les garanties minimales sont selon lui suffisamment solides et résistantes à l'épreuve du temps. Il plaide que les exigences supplémentaires proposées par la requérante – en particulier l'obligation de démontrer l'existence d'un « soupçon raisonnable » – réduiraient de manière inacceptable l'effectivité des services de renseignement sans offrir une protection supplémentaire significative des droits fondamentaux de l'individu.

231. Par ailleurs, il considère qu'il reste pertinent de distinguer les données de contenu des données de communication, en ce que le contenu est susceptible d'être plus sensible que les données de communication. Il

souscrit à la conclusion de la chambre selon laquelle il serait faux de présumer automatiquement que les interceptions en masse constituent une plus grande intrusion dans la vie privée d'un individu que les interceptions ciblées puisqu'une fois qu'une interception ciblée a été mise en place, il est probable que toutes les communications interceptées, ou presque toutes, seront analysées, ce qui n'est pas le cas avec les interceptions en masse, où les restrictions apportées à l'examen et à l'utilisation des données déterminent le degré d'atteinte aux droits fondamentaux de l'individu.

232. Il affirme, enfin, que toute obligation d'expliquer ou de justifier dans l'autorisation les sélecteurs ou les critères de recherche utilisés restreindrait gravement l'effectivité de l'interception en masse, compte tenu du degré élevé d'incertitude quant à la source de la menace. Il plaide qu'une supervision *a posteriori* offre des garanties suffisantes.

d) Le gouvernement du Royaume de Norvège

233. Le gouvernement norvégien soutient que la marge d'appréciation dont jouissent les États pour instaurer et mettre en œuvre un régime d'interception en masse à des fins de sécurité nationale doit être large car les services de renseignement doivent pouvoir s'adapter à l'évolution rapide des technologies de l'information et de la communication. Il explique que les acteurs hostiles changent d'appareils et d'identité numérique à un tel rythme qu'il est difficile de les suivre dans le temps. Il ajoute qu'il est également difficile de découvrir et de contrecarrer les cyberopérations hostiles en temps utile sans disposer d'outils permettant de découvrir les anomalies et les signatures pertinentes. Il ne fait donc aucun doute, selon lui, que le recours à des moyens modernes tels que l'interception en masse est nécessaire pour repérer des menaces encore inconnues dans le domaine numérique et pour permettre aux services de détecter et de suivre les menaces en matière de renseignement pertinentes.

234. Il en tire la conclusion que la Cour devrait fonder son contrôle sur une appréciation globale du caractère suffisant et adéquat des garanties procédurales mises en place contre les abus et se garder d'énumérer des impératifs catégoriques. Il plaide également que la Cour ne devrait pas appliquer des critères qui amoindriraient indirectement l'ample marge d'appréciation dont jouissent les États pour décider de mettre en œuvre un régime d'interception en masse à des fins de sécurité nationale. Or, estime-t-il, les critères du « soupçon raisonnable » ou de la « notification subséquente » auraient cet effet.

235. Le gouvernement norvégien engage enfin la Cour à s'abstenir d'importer des notions et des critères issus de la jurisprudence de la CJUE. Il rappelle tout d'abord qu'à l'époque des faits, dix-neuf des États membres du Conseil de l'Europe n'étaient pas membres de l'Union européenne. Il argue ensuite que si la Convention et la Charte des droits fondamentaux présentent de nombreuses similitudes, il existe entre ces deux textes des

différences, en particulier à l'article 8 de la Charte, qui garantit un droit à la protection des données à caractère personnel. Il ajoute enfin que la notion de « proportionnalité » n'est pas identique dans la jurisprudence de la CJUE, où elle s'apprécie à l'aune de la « stricte nécessité », et dans la jurisprudence de la Cour.

4. Appréciation de la Cour

a) Observations liminaires

236. 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.

237. 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

238. Le Gouvernement soutient que la requérante n'a subi aucune ingérence dans l'exercice de ses droits protégés par l'article 8. À cet égard, il argue que, d'une part, elle n'appartient pas à un groupe de personnes ou d'entités visées par la législation pertinente et il est hautement improbable que ses communications fassent l'objet d'un examen analytique et, d'autre part, les stades antérieurs de l'interception en masse de communications telle qu'elle est opérée en Suède ne constituent pas une ingérence dans l'exercice des droits protégés par l'article 8.

239. 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.

240. 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.

241. 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.

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

243. 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.

244. La Cour considère que l'article 8 s'applique à chacune des étapes décrites ci-dessus. Si l'interception intiale 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 (*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 des 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 (paragraphes 86-91 ci-dessus).

245. 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 suédois pertinent 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

246. 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*, précité, § 130). 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 c. Roumanie* [GC], n° 28341/95, § 52, CEDH 2000-V, *S. et Marper*, précité, § 95, et *Kennedy*, précité, § 151).

247. 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 c. Royaume-Uni*, 2 août 1984, § 67, série A n° 82, *Leander*, précité, § 51, *Huvig c. France*, 24 avril 1990, § 29, série A n° 176-B, *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, et *Weber et Saravia*, décision précitée, § 94).

248. 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).

249. 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 : 1) la nature des infractions susceptibles de donner lieu à un mandat d'interception ; 2) la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ; 3) la limite à la durée d'exécution de la mesure ; 4) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; 5) les précautions à prendre pour la communication des données à d'autres parties ; et 6) les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites (*Huvig*, précité, § 34, *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).

250. 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*, précité, §§ 55 et 56).

251. 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 (*Roman Zakharov*, précité, § 234 ; voir aussi *Kennedy*, précité, § 167).

252. 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).

253. 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

254. 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, 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.

255. 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. 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. Par conséquent, l'étendue de l'activité de surveillance examinée dans ces deux affaires aurait été bien plus restreinte.

256. Il en va de même pour les données de communication associées. 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. 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.

257. 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.

258. 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 137 ci-dessus).

259. 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 131-146 ci-dessus).

260. 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.

261. 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 239 ci-dessus.

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

262. 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 249 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.

263. 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.

264. 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 86 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).

265. Pour ce qui est, tout d'abord, de l'autorisation, la Grande Chambre considère que si l'autorisation judiciaire constitue une « importante garantie contre l'arbitraire », elle n'est pas une « exigence nécessaire ». L'interception en masse devrait néanmoins être autorisée par un organe indépendant, c'est-à-dire un organe indépendant du pouvoir exécutif.

266. 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.

267. 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. La Cour note toutefois que le gouvernement néerlandais a soutenu, dans sa tierce intervention, 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 228-232 ci-dessus). Au Royaume-Uni, l'IPT a jugé 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 » (*Big Brother Watch et autres*, précité, § 49).

268. Compte tenu des caractéristiques de l'interception en masse (paragraphes 258 et 259 ci-dessus), du grand nombre de sélecteurs employés 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.

269. 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.

270. 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.

271. 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).

272. 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.

273. 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).

274. 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 264 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).

275. Pour déterminer si l'État défendeur a agi dans les limites de sa marge d'appréciation (paragraphe 256 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 », en vertu de 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.

276. 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 des 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.

277. Pour les raisons exposées au paragraphe 256 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.

278. 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. 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 liminaires

279. Comme l'a constaté la chambre, les parties ne contestent pas que les activités de ROEM telles qu'elles sont actuellement organisées en Suède ont une base en droit interne (paragraphe 111 de l'arrêt de la chambre). Il n'est pas non plus contesté que le régime de ROEM litigieux poursuit des buts légitimes répondant à l'intérêt de la sécurité nationale puisqu'il vise à soutenir la politique étrangère, la politique de défense et la politique de sécurité de la Suède et à repérer les menaces extérieures qui pèsent sur le pays. Selon l'approche exposée ci-dessus, il reste donc à vérifier si le droit interne était accessible lorsque la chambre a examiné l'affaire et s'il contenait des garanties et des garde-fous effectifs et suffisants pour

satisfaire aux exigences de « prévisibilité » et de « nécessité dans une société démocratique ».

280. L'interception en masse de signaux électroniques aux fins du renseignement extérieur est encadrée en Suède par différents textes législatifs, dont les principaux sont la loi relative au renseignement extérieur et l'ordonnance qui y est associée, la loi et l'ordonnance relatives au renseignement d'origine électromagnétique, la loi sur le tribunal pour le renseignement extérieur, ainsi que la loi et l'ordonnance sur le traitement des données à caractère personnel dans le cadre des activités du FRA. D'autres dispositions pertinentes concernant, en particulier, certains aspects du fonctionnement des mécanismes de supervision et des recours applicables se trouvent dans l'ordonnance portant instructions pour l'Inspection du renseignement extérieur, la loi portant instructions pour les médiateurs parlementaires et la loi sur la supervision assurée par le chancelier de la Justice (paragraphes 14-74 ci-dessus).

281. Il n'est pas contesté que toutes ces dispositions sont accessibles au public. Partant, la Cour admet que le droit interne est suffisamment « accessible ».

282. Pour ce qui est de la question de savoir si le droit interne contient 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 aux paragraphes β) à ι) ci-dessous chacune des huit exigences énoncées au paragraphe 275 ci-dessus.

283. Dans la présente affaire, elle examinera en même temps les exigences concernant l'interception du contenu de communications électroniques et les exigences concernant l'interception des données de communication associées. Cette approche est justifiée par le fait, non contesté par les parties, qu'en vertu du régime suédois de ROEM, les mêmes dispositions, procédures et garanties relatives à l'interception de signaux électroniques et à la conservation, à l'examen, à l'utilisation et au stockage des éléments ainsi obtenus s'appliquent indistinctement aux données de communication et au contenu des communications. Le régime suédois ne soulève donc aucune question distincte concernant l'utilisation des données de communication dans les opérations d'interception en masse.

2) Les motifs pour lesquels l'interception en masse peut être autorisée

284. Comme l'a relevé la chambre, la loi relative au renseignement d'origine électromagnétique dispose qu'il ne peut être mené d'activités de ROEM qu'afin de recueillir des informations :

1. sur des menaces militaires extérieures pesant sur le pays ;
2. sur les conditions de la contribution de la Suède à des missions internationales humanitaires ou de maintien de la paix ou sur les menaces qui pourraient peser sur des intérêts suédois dans le cadre de telles opérations ;

3. sur le contexte stratégique en matière de terrorisme international ou d'autres formes graves de criminalité transfrontière risquant de menacer des intérêts nationaux essentiels ;
4. sur le développement et la prolifération d'armes de destruction massive, d'équipements militaires ou d'autres produits similaires déterminés ;
5. sur des risques extérieurs menaçant gravement l'infrastructure sociale ;
6. sur des conflits à l'étranger susceptibles d'avoir des répercussions sur la sécurité internationale ;
7. sur des opérations de services de renseignement étrangers dirigées contre des intérêts suédois ; et
8. sur les actes ou les intentions d'une puissance étrangère qui revêtent une importance particulière pour la politique étrangère, la politique de défense ou la politique de sécurité de la Suède (paragraphe 22 ci-dessus).

285. Les travaux préparatoires de la loi relative au renseignement d'origine électromagnétique détaillent ces huit buts (paragraphe 23 ci-dessus). De l'avis de la Cour, le niveau de détail et les termes employés délimitent avec une clarté suffisante le domaine dans lequel il peut être recouru à l'interception en masse, compte tenu notamment du fait que le régime litigieux vise à détecter des menaces extérieures inconnues dont la nature peut varier et évoluer avec le temps.

286. La Cour observe que si l'article 4 de la loi relative au renseignement extérieur exclut que les activités de ROEM menées dans le cadre du renseignement extérieur puissent servir à accomplir des missions de répression ou de prévention des infractions, l'un des huit buts énumérés ci-dessus concerne les « formes graves de criminalité transfrontière », telles que, selon les travaux préparatoires, « le trafic de stupéfiants ou la traite d'êtres humains, susceptibles par leur échelle de menacer d'importants intérêts nationaux » (paragraphe 23 ci-dessus).

287. Les travaux préparatoires précisent que l'objectif poursuivi à cet égard est la collecte d'informations stratégiques sur le terrorisme ou d'autres formes graves de criminalité transfrontière du point de vue de la politique étrangère et de la politique de sécurité de la Suède, et non la lutte opérationnelle contre l'activité criminelle (*ibidem*). Il est incontesté que les informations obtenues dans le cadre du régime de ROEM litigieux ne peuvent pas être utilisées dans le cadre d'une procédure pénale. Comme l'a expliqué le Gouvernement, aucune directive d'attribution de tâches de ROEM ne peut être émise pour enquêter sur des infractions pénales et, lorsque le FRA transmet des renseignements à d'autres services, il précise qu'ils ne peuvent être utilisés dans le cadre d'une enquête pénale. Au vu de ce qui précède, la Cour ne partage pas les préoccupations exprimées par la requérante quant au fait que certains services de police peuvent depuis le

1er mars 2018 adopter des directives d'attribution de tâches pour des activités de ROEM et que la Sûreté peut se voir accorder un accès direct aux éléments analysés du FRA (paragraphes 193 *in fine* et 196 *in fine* ci-dessus). À cet égard, elle juge convaincantes les précisions apportées par le Gouvernement, qui a expliqué que ces deux autorités peuvent seulement accéder à des « données qui constituent des résultats d'analyse » afin d'opérer des évaluations stratégiques, et que l'interdiction d'avoir recours au ROEM, branche du renseignement extérieur, aux fins d'une enquête pénale est pleinement appliquée (paragraphe 214 ci-dessus).

288. En bref, les motifs pour lesquels l'interception en masse peut être autorisée en Suède sont clairement délimités de manière à permettre le contrôle nécessaire au stade de l'autorisation et lors de la phase opérationnelle, ainsi que la supervision *a posteriori*.

3) Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées

289. Dans un système d'interception en masse, les circonstances dans lesquelles les communications peuvent être interceptées sont très larges, puisque ce sont les canaux de transmission qui sont ciblés, plutôt que les appareils à partir desquels les communications sont envoyées ou que les expéditeurs et les destinataires des communications. Les circonstances dans lesquelles les communications peuvent être examinées sont plus restreintes, mais elles s'appliquent néanmoins à un nombre de communications relativement important par rapport à celui des communications examinées dans le cadre d'une interception ciblée, puisque l'interception en masse peut être utilisée pour la poursuite de buts plus variés et que la sélection des communications en vue de leur examen est fonction de critères autres que celui de l'identité de l'expéditeur ou du destinataire.

290. Pour ce qui est de l'interception, les activités de ROEM menées sur des signaux transmis par fibre optique ne peuvent concerner que les communications traversant la frontière suédoise. Par ailleurs, les communications entre un émetteur et un destinataire qui se trouvent tous deux en Suède ne peuvent pas être interceptées, que la transmission ait lieu par la voie aérienne ou par câble (paragraphe 25 ci-dessus). Le Gouvernement a toutefois admis qu'il n'est pas toujours possible de séparer les communications « intérieures » des communications « extérieures » aux premiers stades de l'interception, comme le comité sur le renseignement d'origine électromagnétique l'a confirmé dans son rapport de 2011 (paragraphes 77-80 ci-dessus ; voir également les rapports de l'autorité de protection des données, aux paragraphes 75-76 ci-dessus).

291. Il est vrai que le FRA peut également intercepter, dans le cadre de ses activités de développement, des signaux contenant des données non pertinentes aux fins des activités ordinaires de renseignement extérieur. Il ressort du rapport du comité sur le renseignement d'origine

électromagnétique (paragraphes 77-80 ci-dessus) que les données interceptées dans le cadre des activités de développement du FRA peuvent être utilisées, notamment « lues » et conservées, à des fins de développement technologique, qu'elles relèvent ou non de l'une des catégories définies dans le cadre des huit buts du renseignement extérieur.

292. La Cour observe toutefois que l'intérêt pour les autorités des signaux interceptés dans le contexte des activités de développement du FRA ne réside pas dans les données qu'ils peuvent contenir mais uniquement dans la possibilité qu'ils offrent d'analyser les systèmes et les voies par lesquels les informations sont transmises. Elle juge satisfaisante l'explication donnée par le gouvernement défendeur quant à la nécessité d'un tel dispositif (paragraphe 207 ci-dessus). Les exemples fournis (la nécessité de surveiller le trafic entre certains pays afin de déterminer les canaux par lesquels transite le trafic pertinent, la nécessité de repérer de nouvelles tendances telles que de nouveaux types de signaux ou de protection des signaux) paraissent convaincants : les autorités doivent être en mesure de réagir à l'évolution des pratiques en matière de technologie et de communication et, pour cette raison, elles peuvent avoir besoin de surveiller de très larges segments du trafic international de signaux. L'atteinte aux droits protégés par l'article 8 qu'engendre de telles activités paraît très faible compte tenu du fait que les données ainsi obtenues ne sont pas sous une forme destinée à générer du renseignement.

293. Il est de surcroît incontesté que les informations qui pourraient ressortir des signaux interceptés à des fins de développement technologique ne peuvent être utilisées dans le cadre des activités de renseignement que de manière conforme aux huit buts fixés par la loi et aux directives d'attribution de tâches pertinentes (paragraphe 79 ci-dessus). Par ailleurs, les activités de développement requièrent une autorisation délivrée par le tribunal pour le renseignement extérieur et sont soumises à la supervision de l'Inspection, notamment quant au respect de la loi et des directives d'attribution de tâches approuvées par le tribunal pour le renseignement extérieur. Dans ces conditions, la Cour estime que le cadre juridique dans lequel sont menées les activités de développement du FRA renferme des garanties propres à prévenir les tentatives de contournement des restrictions légales relatives aux motifs pour lesquels le ROEM peut être utilisé.

294. Au vu de ce qui précède, la Cour peut admettre que les dispositions juridiques relatives à l'interception en masse en Suède définissent avec une clarté suffisante les circonstances dans lesquelles des communications peuvent être interceptées.

4) La procédure d'octroi d'une autorisation

295. En vertu du droit suédois, toute mission de ROEM menée par le FRA doit être au préalable autorisée par le tribunal pour le renseignement extérieur. Le FRA peut accorder lui-même une autorisation si le fait de

demander l'autorisation au tribunal risque d'engendrer des délais ou d'autres obstacles susceptibles d'avoir un impact d'une importance essentielle sur la réalisation de l'un des buts spécifiés du ROEM. Il doit alors en informer immédiatement le tribunal. Celui-ci statue sans délai sur l'autorisation ; il peut l'annuler ou la modifier si nécessaire (paragraphes 30-33 ci-dessus).

296. Il ne fait aucun doute que le tribunal pour le renseignement extérieur satisfait à l'exigence d'indépendance par rapport au pouvoir exécutif. En particulier, son président et ses vice-présidents sont des juges permanents ; tous ses membres sont certes nommés par le gouvernement, mais pour un mandat dont la loi fixe la durée à quatre ans. Il est par ailleurs incontesté que ni le gouvernement ni le parlement ni aucune autre autorité ne peuvent intervenir dans la décision du tribunal, laquelle est juridiquement contraignante.

297. Comme l'a constaté la chambre, le secret fait que le tribunal pour le renseignement extérieur n'a jamais tenu aucune audience publique et que toutes ses décisions sont confidentielles. Le droit suédois prévoit toutefois la présence obligatoire d'un représentant chargé de la protection de la vie privée aux audiences de ce tribunal, sauf en cas d'urgence. Ce représentant, qui doit être ou avoir été juge ou avocat, agit de manière indépendante. Il ne représente pas la personne concernée par une mesure de renseignement mais défend l'intérêt public. Il a accès à tout le dossier de l'affaire et peut faire des déclarations (paragraphe 34 ci-dessus). De l'avis de la Cour, compte tenu de la nécessité impérative de maintenir le secret, en particulier au stade de l'autorisation initiale et pendant le déroulement des activités de ROEM, le dispositif décrit ci-dessus contient des garanties pertinentes contre l'arbitraire et doit être considéré comme une limitation inévitable à la transparence de la procédure d'autorisation.

298. La Cour observe par ailleurs que lorsqu'il demande une autorisation, le FRA doit préciser pourquoi les renseignements recherchés sont nécessaires, et quels sont les canaux de transmission auxquels il a besoin d'accéder et les sélecteurs – ou au moins les catégories de sélecteurs – qu'il entend utiliser. Ces éléments devraient permettre de déterminer si la mission est conforme à la législation applicable, notamment aux huit buts pour lesquels des activités de ROEM peuvent être menées, et si les renseignements qu'elle permettra de recueillir justifient l'atteinte à la vie privée qui en résulte (paragraphes 30-33 ci-dessus).

299. Il est à noter que l'article 3 de la loi relative au renseignement d'origine électromagnétique exige que les sélecteurs soient formulés de manière à limiter autant que possible les atteintes à l'intégrité personnelle (paragraphe 26 ci-dessus), ce qui suppose une analyse de la nécessité et de la proportionnalité. L'examen de la conformité à cette exigence au stade de l'autorisation relève de la compétence du tribunal pour le renseignement extérieur. Cette juridiction adopte, au terme d'une procédure à laquelle

participe un représentant chargé de la protection de la vie privée, une décision contraignante. Il y a là une garantie importante prévue par le système suédois d'interception en masse.

300. La Cour observe par ailleurs que le droit suédois prévoit une forme d'autorisation préalable spéciale des sélecteurs forts puisque le tribunal pour le renseignement intérieur vérifie si, comme l'exige l'article 3 de la loi relative au renseignement d'origine électromagnétique, l'utilisation de sélecteurs se rapportant directement à une personne physique donnée revêt une « importance exceptionnelle » pour les activités de renseignement. Aucune explication n'a été produite devant la Cour quant à l'interprétation de cette disposition dans la pratique du tribunal pour le renseignement extérieur ni quant à la manière dont l'article 3 s'articule avec l'article 5 de la même loi, selon lequel l'autorisation judiciaire peut, au moins dans certains cas, porter sur des « catégories de sélecteurs » plutôt que sur des sélecteurs individuels. La question se pose ainsi de savoir si, dans ce cas, c'est-à-dire lorsque des sélecteurs individuels n'auraient pas été approuvés par le tribunal pour le renseignement extérieur, on pourrait considérer qu'il existe une procédure d'autorisation interne préalable comportant une vérification distincte et objective (paragraphe 269 ci-dessus). Toutefois, compte tenu de l'indépendance du tribunal pour le renseignement extérieur et des garanties procédurales applicables à la procédure menée devant lui, le critère de l'« importance exceptionnelle » au stade de l'autorisation est de nature à offrir une protection renforcée pertinente contre l'utilisation arbitraire de sélecteurs se rapportant à une personne donnée.

301. Le système suédois d'autorisation a ses limites. Par exemple, il peut être difficile pour le tribunal pour le renseignement extérieur d'apprécier la question de la proportionnalité lorsque la demande d'autorisation formulée par le FRA indique seulement des catégories de sélecteurs, qu'elle en indique plusieurs milliers ou que les sélecteurs sont exprimés sous forme de combinaisons techniques de chiffres et de lettres.

302. Aux fins de l'examen de la Cour, l'élément à retenir à ce stade est toutefois que le système suédois d'autorisation offre un contrôle juridictionnel en amont des demandes d'autorisation qui est étendu – en ce sens que le tribunal examine le but de la mission, les canaux de transmission et les catégories de sélecteurs qui seront utilisés – et dans le cadre duquel le juge vérifie suffisamment en détail la régularité des activités secrètes d'interception en masse de données aux fins du ROEM menées dans le cadre du renseignement extérieur. Ce contrôle constitue une garantie importante, notamment contre la mise en œuvre d'opérations d'interception en masse abusives ou clairement disproportionnées. Caractéristique importante, il définit également le cadre dans lequel une opération concrète doit se dérouler et les limites dont le respect fait ensuite l'objet de la supervision et des mécanismes de contrôle *a posteriori* applicables.

5) Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés

303. Il ressort des éléments dont dispose la Cour qu'en Suède l'interception des signaux transmis par câble est automatisée, alors qu'elle peut être automatisée ou manuelle lorsqu'il s'agit de signaux transmis par la voie aérienne. Lorsqu'il est automatisé, le processus d'interception des signaux transmis par voie aérienne est identique au processus d'interception des signaux transmis par des câbles transfrontaliers.

304. En ce qui concerne l'interception et les recherches non automatisées de signaux électroniques transmis par voie aérienne, le gouvernement suédois a précisé devant la Grande Chambre qu'elles sont utilisées principalement pour rendre compte pratiquement en temps réel d'activités militaires étrangères et qu'elles sont effectuées par un opérateur qui écoute en temps réel les transmissions radio militaires sur des radiofréquences sélectionnées ou qui visualise sur un écran l'énergie d'un signal sous forme électronique, avant d'enregistrer les parties pertinentes, qui seront ensuite utilisées pour établir des analyses et des rapports. La requérante n'a pas fait de commentaires en réponse.

305. Même en admettant que l'interception de radiofréquences militaires étrangères puisse, dans de rares cas, porter atteinte à des droits protégés par l'article 8, la Cour observe que cet aspect du régime suédois de ROEM est soumis aux mêmes procédures et garanties que celles applicables à l'interception et à l'utilisation des communications transmises par câble.

306. Pour en revenir à la procédure d'examen des éléments interceptés, la Cour observe que, comme l'a expliqué le gouvernement défendeur, le FRA procède à un traitement automatique et manuel des données qui peut prendre la forme, par exemple, d'une cryptanalyse, d'une structuration ou encore d'une traduction. Les informations traitées sont ensuite étudiées par un analyste dont la tâche consiste à y repérer les éléments utiles pour le renseignement. L'étape suivante consiste en l'élaboration d'un rapport de renseignement extérieur qui est distribué à des destinataires précis (paragraphes 18 et 29 ci-dessus).

307. La Cour juge important qu'au stade de l'examen le FRA soit tenu d'écarter immédiatement les communications intérieures interceptées dès qu'elles ont été identifiées comme telles (paragraphe 38 ci-dessus).

308. Même si la distinction entre communications intérieures et communications extérieures n'est pas toujours étanche et si l'interdiction d'intercepter les communications intérieures ne semble pas pouvoir empêcher que cela se produise au stade de l'interception automatique de signaux, l'exclusion du trafic intérieur du champ du ROEM doit être considérée comme une limitation importante de la marge de manœuvre des autorités et une garantie contre les abus. Cette limitation définit le cadre dans lequel les autorités sont habilitées à agir et offre aux mécanismes existants d'autorisation préalable, de supervision et de contrôle un critère

important pour l'appréciation de la légalité de l'opération et la protection des droits des individus. Il est clair en particulier que le choix des canaux de transmission et des catégories de sélecteurs – qui fait l'objet d'un contrôle du tribunal pour le renseignement extérieur (paragraphe 30 ci-dessus) – doit être conforme à l'exclusion susmentionnée des communications intérieures.

309. Comme cela a déjà été observé (paragraphe 300 ci-dessus), la pratique du tribunal pour le renseignement extérieur en ce qui concerne l'autorisation préalable des sélecteurs ou catégories de sélecteurs se rapportant directement à des personnes identifiables n'a pas été exposée devant la Cour. Celle-ci note toutefois que le Gouvernement affirme que le FRA conserve systématiquement des journaux d'historique et des archives retraçant tout le déroulement du processus, depuis la collecte des données jusqu'au rapport final, en passant par la communication à des tiers et la destruction des données. Toutes les recherches effectuées par des analystes sont consignées. Lorsque la recherche est faite dans une compilation de données qui contient des données à caractère personnel, l'archive indique les sélecteurs utilisés, l'heure, le nom de l'analyste et le motif justifiant la recherche, notamment la directive détaillée d'attribution de tâches dont elle relève. Le FRA conserve non seulement les journaux d'historique, mais aussi des archives où sont consignées les décisions prises au cours du processus de ROEM.

310. La requérante ne conteste pas ce qui précède mais soutient, premièrement, qu'il n'a pas été démontré que les journaux d'historique soient suffisamment détaillés et, deuxièmement, que, n'étant pas prévues par la loi, les pratiques de tenue des archives du FRA dépendent entièrement des procédures internes et du pouvoir d'appréciation de cet organisme.

311. La Cour considère que l'obligation de conserver les journaux d'historique et une archive détaillée de chaque étape des opérations d'interception en masse, y compris l'ensemble des sélecteurs utilisés, doit être énoncée dans le droit national. Le fait qu'elle ne figure en Suède que dans des instructions internes est indubitablement une carence. Toutefois, compte tenu, notamment, de l'existence de mécanismes de contrôle applicables à tous les aspects des activités du FRA, il n'y a pas de raison de considérer qu'il n'est pas conservé en pratique des journaux d'historique et des archives détaillés ou que le FRA pourrait modifier arbitrairement ses instructions internes et supprimer ainsi son obligation à cet égard. S'il est vrai qu'en 2010 et en 2016 l'autorité suédoise de protection des données a critiqué un aspect des pratiques du FRA concernant la conservation des journaux d'historique, cette critique ne portait que sur la manière dont l'organisme contrôlait les journaux d'historique afin de détecter l'utilisation injustifiée de données à caractère personnel (paragraphe 76 ci-dessus). Par ailleurs, le Gouvernement a précisé que, depuis le 1er janvier 2018, les journaux d'historique, qui étaient auparavant conservés par des « responsables de système » individuels au sein du FRA, sont désormais

envoyés à un groupe fonctionnel central, ce qui permet une meilleure surveillance. Cette modification a été portée à la connaissance de l'autorité suédoise de protection des données, qui a classé le dossier sans demander la prise d'autres mesures.

312. Le droit suédois offre une protection spécifique pour les données à caractère personnel, notamment les données susceptibles de révéler certains aspects de la vie privée ou des communications de personnes physiques. Dans le contexte du ROEM, la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA fait peser sur celui-ci l'obligation de veiller à ce que les données personnelles ne soient collectées que dans des buts expressément autorisés par les directives d'attribution de tâches et dans les limites de l'autorisation accordée par le tribunal pour le renseignement extérieur. Comme l'a noté la chambre, les données personnelles traitées doivent également être adéquates et pertinentes au regard de la finalité du traitement. Il ne peut être traité plus de données personnelles que nécessaire pour atteindre le but visé. Toutes les mesures raisonnables doivent être prises pour corriger, bloquer et détruire complètement les données personnelles incorrectes ou incomplètes au regard de la finalité (paragraphe 40 ci-dessus). Les employés du FRA qui traitent des données à caractère personnel sont soumis à une procédure officielle d'habilitation de sécurité et à une obligation de confidentialité. Ils sont tenus de gérer les données personnelles de manière sûre et s'exposent à des sanctions pénales s'ils ne s'acquittent pas correctement des tâches relatives au traitement des données à caractère personnel (paragraphe 42 ci-dessus).

313. La requérante critique le fait que les garanties mentionnées au paragraphe précédent ne s'appliquent qu'aux éléments interceptés qui contiennent des « informations se rapportant directement ou indirectement à une personne physique vivante ». Elle en déduit que les personnes morales ne bénéficient d'aucune protection.

314. La Cour observe toutefois que rien ne laisse penser que la protection offerte par la loi et l'ordonnance sur le traitement des données à caractère personnel dans le cadre des activités du FRA ne s'applique pas au contenu des communications échangées par des personnes morales telles que la requérante lorsque ces communications contiennent des « informations se rapportant directement ou indirectement à une personne physique vivante ». Il convient, par ailleurs, de noter que la plupart des obligations et garanties imposées par la législation susmentionnée n'ont normalement de valeur que pour les personnes physiques. Par exemple, la loi en question interdit de traiter les données à caractère personnel uniquement sur la base des informations concernant la race ou l'origine ethnique de la personne, ses convictions politiques, religieuses ou philosophiques, son appartenance à un syndicat, son état de santé ou sa sexualité. Elle prévoit une obligation spécifique limitant la conservation

d'éléments contenant des données à caractère personnel, ainsi que des sanctions en cas de mauvaise gestion de ces données. Elle garantit une surveillance particulière du traitement des données à caractère personnel et définit les pouvoirs de l'autorité de protection des données à cet égard. En d'autres termes, cette loi ajoute aux garanties qui sont déjà applicables aux informations concernant tant les personnes physiques que les personnes morales un niveau de protection supplémentaire, adapté aux spécificités des données à caractère personnel.

315. Cette approche, qui tient compte de la sensibilité particulière des données à caractère personnel, ne semble pas problématique et ne signifie pas que les communications des personnes morales ne sont protégées par aucune garantie. Contrairement à ce que soutient la requérante, rien dans la législation pertinente ne laisse penser que les éléments interceptés qui ne contiennent pas de données à caractère personnel puissent être utilisées dans un but incompatible avec le but initial de l'interception, tel qu'approuvé par le tribunal pour le renseignement extérieur.

316. En somme, la Cour estime que la législation relative à la sélection, l'examen et l'utilisation des données interceptées prévoit des garanties adéquates contre le risque d'abus portant atteinte aux droits protégés par l'article 8.

6) Les précautions à prendre pour la communication des données à d'autres parties

317. Pour ce qui est de la communication de données par le FRA à d'autres autorités suédoises, la Cour observe que l'objectif même du ROEM est d'obtenir des informations utiles pour la mission des services de l'État correspondants. Le cercle des autorités nationales qui peuvent se voir remettre de telles informations en Suède est restreint et comprend surtout la Sûreté et les forces armées. Le FRA peut donner à ces deux autorités un accès direct à des données qui constituent le résultat d'analyses réalisées dans une compilation de données, afin de leur permettre d'opérer des évaluations stratégiques des menaces terroristes. Il le fait en particulier dans le cadre d'un groupe de travail tripartite, le Centre national d'évaluation des menaces terroristes, composé d'analystes de ses services, de la Sûreté et des forces armées. La Cour considère que le régime décrit ci-dessus est clairement délimité et ne paraît pas générer un risque d'abus particulier.

318. La Cour note par ailleurs que la chambre a exprimé des préoccupations quant au dispositif suédois de communication de données à d'autres États ou à des organisations internationales, à trois égards : a) le fait que la législation n'impose pas de tenir compte, lorsqu'est prise la décision de communication des données, du préjudice que cela pourrait causer à l'individu concerné, b) l'absence de disposition obligeant l'État ou l'organisation destinataire à protéger les données par des garanties identiques ou similaires à celles applicables en droit suédois, et c) la

latitude relativement importante laissée à l'État par la possibilité de communiquer des données lorsque cette démarche est nécessaire à la « coopération internationale en matière de défense et de sécurité ». La chambre a néanmoins considéré que les mécanismes de supervision existants contrebalançaient de manière suffisante ces lacunes du cadre juridique (paragraphe 150 de l'arrêt de la chambre).

319. Devant la Grande Chambre, le Gouvernement conteste essentiellement l'existence de motifs de préoccupation, arguant que la coopération internationale est limitée aux échanges avec des partenaires étrangers fiables et qu'elle est contrôlée par l'Inspection, alors que la requérante soutient que la latitude accordée au FRA est trop large et que les mécanismes de supervision existants ne contrebalancent pas les lacunes constatées, compte tenu de l'absence d'obligations juridiques dont le respect pourrait être contrôlé (voir le détail des positions des parties aux paragraphes 200, 201, 215 et 216 ci-dessus).

320. La Cour souligne d'emblée qu'en l'espèce, il ne s'agit pas de statuer sur un cas concret, tel un cas de divulgation ou d'utilisation par une organisation ou un gouvernement étranger de données à caractère personnel qui lui auraient été transmises par les autorités suédoises. Aucun exemple de ce type n'a d'ailleurs été produit devant elle. Toutefois, dans la mesure où la possibilité de transmettre des renseignements à des tiers étrangers est présente dans les activités et le régime suédois d'interception en masse dont l'existence même peut être considérée comme une ingérence dans l'exercice des droits protégés par l'article 8, la Cour doit, eu égard aux griefs de la requérante, vérifier la conformité du régime suédois de transmission de renseignements et de son fonctionnement aux exigences de qualité de la loi et de nécessité dans une société démocratique. Elle note que les griefs de la requérante ne portent que sur l'envoi de renseignements à des tiers étrangers et ne concernent pas la réception de renseignements de l'étranger et leur utilisation par les autorités suédoises.

321. Il est incontesté que diverses raisons peuvent conduire les États contractants à devoir transmettre à des services étrangers des renseignements obtenus par l'interception en masse de communications. Il peut s'agir, par exemple, d'avertir des gouvernements étrangers de menaces existantes, de solliciter leur aide pour repérer et affronter ces menaces, ou encore de permettre à des organisations internationales d'exercer leur mandat. La coopération internationale est essentielle pour l'efficacité des efforts déployés par les autorités pour détecter et contrecarrer les menaces potentielles à la sécurité nationale des États contractants.

322. La Cour observe que la possibilité pour le FRA de transmettre à des partenaires étrangers les renseignements qu'il a recueillis est prévue par le droit suédois, qui définit également le but général de cette transmission (paragraphes 49 et 74 ci-dessus). Il convient de relever, toutefois, que le niveau de généralité des termes employés ne peut qu'amener à conclure que

le FRA peut envoyer des renseignements à l'étranger dès lors que cette transmission est considérée comme étant dans l'intérêt du pays.

323. Compte tenu du caractère imprévisible des situations susceptibles de justifier une coopération avec des services de renseignement étrangers, il est compréhensible que l'étendue précise du partage de renseignements ne puisse être délimitée par un texte qui établirait, par exemple, des listes exhaustives et détaillées des situations, types de renseignements ou contenus susceptibles d'être partagés. Le cadre et la pratique juridiques applicables doivent toutefois opérer d'une manière propre à limiter le risque d'abus et d'atteinte disproportionnée aux droits protégés par l'article 8.

324. À cet égard, la Cour observe, tout d'abord, que dans la mesure où les renseignements transmis à des services étrangers sont des informations que le FRA a obtenues dans le cadre de ses activités d'interception en masse, ils sont nécessairement le produit de procédures régies par la loi auxquelles s'appliquent toutes les garanties pertinentes : d'une part, les garanties procédurales, dont l'octroi d'une autorisation par le tribunal pour le renseignement extérieur et la supervision par l'Inspection (paragraphes 295-302 ci-dessus et 345-353 ci-dessous), et d'autre part, les restrictions matérielles, notamment celles relatives aux motifs pour lesquels l'interception de signaux peut être ordonnée, aux recherches faites sur les données interceptées, notamment au moyen de sélecteurs identifiant un individu, et à tout examen ultérieur (paragraphes 284-288 et 303-316 ci-dessus). Comme cela a déjà été exposé, les procédures mentionnées ci-dessus supposent l'appréciation de la nécessité et de la proportionnalité des mesures en cause, notamment au regard des droits protégés par l'article 8 de la Convention. Ainsi, les garanties applicables au niveau national en Suède dans le cadre du processus d'obtention de renseignements qui pourraient ensuite être transmis à des partenaires étrangers limitent également, dans une certaine mesure, le risque que la transmission ait des conséquences négatives.

325. La Cour observe également que les mécanismes de supervision prévus par la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA, mécanismes qui sont spécifiquement adaptés à la protection des données à caractère personnel, s'appliquent à toutes les activités de cet organisme (paragraphe 56 ci-dessus).

326. Elle considère, malgré ce qui précède, que l'absence dans la législation relative au ROEM d'une obligation expresse qui imposerait au FRA d'apprécier la nécessité et la proportionnalité du partage de renseignements au regard de son possible impact sur les droits garantis par l'article 8 est une importante lacune du régime qui régit en Suède les activités d'interception en masse. Il apparaît qu'en conséquence de cet état du droit, le FRA n'est tenu de prendre aucune mesure même lorsque, par exemple, des informations compromettant gravement le droit à la vie privée sont transmises à l'étranger alors que cela ne présente aucun intérêt

particulier pour le renseignement. Par ailleurs, alors même que les autorités suédoises perdent, évidemment, le contrôle des éléments partagés une fois qu'elles les ont transmis, aucune obligation juridiquement contraignante n'impose au FRA d'analyser les garanties appliquées par le destinataire étranger des renseignements afin de déterminer si elles sont d'un niveau minimum acceptable (paragraphe 276 ci-dessus).

327. La réponse du Gouvernement à ces préoccupations est essentiellement que la coopération avec des services de renseignement étrangers fonctionne inévitablement sur la base d'un intérêt mutuel à la préservation du secret des informations et que cette réalité pratique limite les risques d'abus.

328. La Cour estime que cet élément constitue une garantie insuffisante. Le Gouvernement n'a indiqué aucun obstacle s'opposant à ce que le droit interne énonce clairement une obligation imposant au FRA ou à une autre autorité compétente de mettre en balance la nécessité de transmettre des renseignements à l'étranger et le besoin de protéger le droit au respect de la vie privée. À titre de comparaison, la Cour observe que le régime applicable au Royaume-Uni, par exemple, pose l'obligation de prendre des mesures raisonnables pour s'assurer que les autorités étrangères continueront d'appliquer 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 (paragraphe 7.5 du code de conduite en matière d'interception de communications en vigueur au Royaume-Uni, cité dans *Big Brother Watch et autres*, précité, § 96).

329. Il est vrai qu'en 2014, l'Inspection a effectué un contrôle général de la coopération du FRA avec ses partenaires étrangers et que, entre 2009 et 2017, elle a inspecté à plusieurs reprises d'autres aspects pertinents de ses activités, notamment le traitement qu'il faisait des données à caractère personnel et la manière dont il communiquait ses rapports (paragraphe 53 ci-dessus). Toutefois, étant donné qu'aucune disposition n'oblige expressément le FRA à prendre en compte les questions liées au respect de la vie privée ou à demander au moins des garanties à cet égard à ses partenaires étrangers avant de leur envoyer des renseignements, il n'est pas déraisonnable de considérer, comme la requérante, que l'Inspection, dont le rôle est d'exercer un contrôle de légalité, n'examine pas le partage de renseignements sous l'angle des risques ou des conséquences disproportionnées qui peuvent en découler pour les droits protégés par l'article 8 de la Convention ; et le gouvernement défendeur n'a pas convaincu la Cour qu'un tel examen soit opéré en pratique sur le fondement, par exemple, de dispositions constitutionnelles ou d'autres dispositions générales relatives aux droits fondamentaux. Il s'ensuit que, contrairement à la chambre, la Grande Chambre ne peut conclure que les lacunes constatées dans le cadre réglementaire sont suffisamment contrebalancées par les mécanismes de supervision prévus par le régime suédois.

330. En bref, le fait que ni la loi relative au renseignement d'origine électromagnétique ni aucun autre texte n'impose de prendre en compte les intérêts liés à la vie privée de l'individu concerné au moment de décider de partager des renseignements constitue une lacune importante du régime suédois, dont la Cour doit tenir compte au moment d'apprécier la compatibilité dudit régime avec l'article 8 de la Convention.

7) Les limites posées à la durée de l'interception et de la conservation des éléments ainsi obtenus, et les circonstances dans lesquelles ceux-ci doivent être effacés ou détruits

331. Il appartient bien entendu aux autorités nationales de décider de la durée des opérations d'interception en masse. Il doit toutefois exister des garanties suffisantes, telles que des indications claires dans le droit interne sur le délai d'expiration de l'autorisation d'interception, les conditions dans lesquelles celle-ci peut être renouvelée et les circonstances dans lesquelles elle doit être annulée (*Roman Zakharov*, précité, § 250).

332. En vertu de l'article 5 a) de la loi relative au renseignement d'origine électromagnétique, une autorisation peut être accordée pour une durée maximale de six mois. Elle peut ensuite être prolongée par périodes de six mois, après réexamen complet de la demande par le tribunal pour le renseignement extérieur, qui vérifie si les conditions pertinentes sont réunies. Comme l'a observé la chambre, la loi suédoise donne donc des indications claires quant au délai d'expiration et aux conditions du renouvellement de l'autorisation.

333. La chambre a toutefois relevé également qu'aucune disposition n'impose au FRA, aux autorités compétentes pour adopter des directives détaillées d'attribution de tâches ou au tribunal pour le renseignement extérieur de mettre fin à une mission de ROEM si les conditions qui la justifiaient ont cessé d'exister ou si les mesures ne sont plus nécessaires.

334. Devant la Grande Chambre, la requérante soutient que l'absence de disposition prévoyant l'annulation d'une autorisation lorsque celle-ci n'est plus nécessaire ouvre la porte à l'exercice pendant plusieurs mois d'une surveillance excessive et inappropriée qui ne cesse pas jusqu'à ce que le mandat arrive à son terme. Elle plaide que cette carence est très importante compte tenu du volume considérable d'informations qui peuvent être obtenues par une interception en masse dans ce laps de temps. Le Gouvernement argue pour sa part qu'il est mis un terme à toute opération d'interception qui n'est plus nécessaire, qui se fonde sur une directive d'attribution des tâches qui a été annulée ou qui n'est pas conforme à l'autorisation dont elle relève.

335. La Cour est d'avis qu'une disposition expresse prévoyant la cessation de toute interception en masse qui n'est plus nécessaire aurait été plus claire que le dispositif existant en Suède selon lequel, semble-t-il, lorsque des circonstances justifiant l'annulation d'une autorisation

apparaissent avant l'expiration de sa validité de six mois, l'autorisation peut être annulée mais ne l'est pas nécessairement.

336. Elle estime toutefois qu'il ne faut pas surestimer l'importance de cette carence, et ce principalement pour deux raisons. Premièrement, le droit suédois prévoit des mécanismes pertinents, tels que la possibilité pour l'autorité dont émane la demande d'annuler une directive d'attribution de tâches ou encore la supervision exercée par l'Inspection, qui peuvent l'une comme l'autre aboutir à la cessation d'une mission d'interception en masse lorsque les conditions qui la justifiaient ont cessé d'exister ou que les mesures ne sont plus nécessaires. Deuxièmement, par la force des choses, dans le contexte des activités de ROEM menées aux fins du renseignement extérieur, la mise en œuvre d'une obligation juridique d'annuler une autorisation qui n'est plus nécessaire doit, selon toute probabilité, largement dépendre d'évaluations opérationnelles internes impliquant le secret. Partant, dans le contexte particulier de l'interception en masse réalisée aux fins du renseignement extérieur, l'existence de mécanismes de supervision ayant accès à toutes les informations internes doit en général être considérée comme offrant des garanties législatives similaires contre les abus relatifs à la durée des opérations d'interception.

337. Pour les raisons exposées ci-dessus, la Cour considère que le droit suédois satisfait aux exigences concernant la durée de l'interception en masse de communications.

338. Pour ce qui est des circonstances dans lesquelles les données interceptées doivent être effacées ou détruites, la chambre est parvenue, aux paragraphes 145 et 146 de son arrêt, aux conclusions suivantes :

> « 145. Contrairement à ce qu'affirme la requérante, plusieurs dispositions réglementent les situations dans lesquelles les données interceptées doivent être détruites, notamment lorsque 1) elles concernent une personne physique déterminée et revêtent une faible importance pour le ROEM, 2) elles sont protégées par les dispositions constitutionnelles relatives au secret protégeant l'anonymat des auteurs et des sources journalistiques, 3) elles contiennent des informations échangées entre un suspect et son avocat, et sont donc protégées par le principe de la confidentialité des échanges entre l'avocat et son client, ou 4) elles contiennent des informations données dans un contexte religieux (confession ou conseil individuel), sauf raisons exceptionnelles justifiant leur examen (...). Par ailleurs, si, malgré l'interdiction de telles interceptions, des communications entre un émetteur et un destinataire qui se trouvent tous deux en Suède ont été interceptées, les données ainsi collectées doivent être détruites dès qu'il apparaît qu'il s'agit de communications internes (...). De même, si une autorisation accordée en urgence par le FRA est annulée ou modifiée par le tribunal pour le renseignement extérieur, tous les renseignements recueillis par des moyens qui ne sont dès lors plus autorisés doivent être immédiatement détruits (...).
>
> 146. Même si le FRA peut tenir des bases de données brutes contenant des informations à caractère personnel pendant un délai maximal d'un an, il convient de garder à l'esprit que les données brutes sont des informations non traitées, c'est-à-dire qu'elles doivent encore être soumises à un traitement manuel. La Cour admet que le FRA a besoin de conserver des données brutes avant qu'elles ne puissent être traitées

> manuellement. Elle souligne toutefois qu'il est important que ces données soient supprimées dès qu'il apparaît qu'elles n'ont plus d'importance aux fins d'une mission de renseignement. »

339. Si la Grande Chambre souscrit en principe à cette analyse, elle estime important de souligner qu'elle ne dispose pas d'informations suffisantes quant à l'application pratique de certains aspects des règles relatives à la destruction des éléments interceptés.

340. Les pouvoirs de supervision de l'Inspection englobent certes le contrôle des pratiques du FRA en matière de destruction des éléments interceptés et cet aspect des activités du FRA a déjà fait l'objet d'inspections (paragraphe 53 ci-dessus). Il s'agit d'une garantie importante de la bonne application des règles existantes.

341. Devant la Grande Chambre, la requérante soutient toutefois que les limites posées à la conservation des éléments interceptés et les exigences concernant leur destruction mentionnées par la chambre ne s'appliquent pas aux éléments qui ne contiennent pas de données à caractère personnel. Le Gouvernement ne s'est pas exprimé sur ce point.

342. La Cour admet qu'il est clairement justifié que des exigences spécifiques s'appliquent à la destruction d'éléments contenant des données à caractère personnel. Pour autant, il faut aussi qu'il existe une règle générale régissant la destruction des autres éléments obtenus au moyen de l'interception en masse de communications lorsque leur conservation peut affecter, par exemple, le droit au respect de la correspondance au sens de l'article 8, y compris celui des personnes morales, telles que la requérante. Au minimum, comme l'a également souligné la chambre, le droit interne devrait imposer d'effacer les données interceptées lorsqu'elles ne sont plus pertinentes aux fins du ROEM. Le Gouvernement n'a pas montré que cette obligation figure dans le cadre réglementaire suédois. Tout en observant que les circonstances dans lesquelles il pourrait se produire qu'aucune des règles spécifiques sur la destruction des éléments interceptés mentionnées dans les paragraphes précédents ne s'applique sont très limitées, la Cour considère toutefois qu'il y a là une lacune procédurale dans le cadre réglementaire.

343. Enfin, la Cour ne dispose pas d'informations suffisantes quant à la manière dont la nécessité de conserver ou de détruire les éléments contenant des données à caractère personnel est appréciée dans la pratique, ni sur le point de savoir si les éléments interceptés non traités sont toujours conservés pendant la durée maximale d'un an ou si la nécessité de leur conservation est régulièrement examinée, comme cela devrait être le cas. Il lui est ainsi difficile d'aboutir à des conclusions exhaustives portant sur tous les aspects de la conservation et de la destruction des éléments interceptés. Elle reviendra lorsqu'elle analysera la question du contrôle *a posteriori* dans le régime suédois d'interception en masse sur la question des conclusions qui peuvent être tirées du fait qu'elle ne dispose pas d'informations

suffisantes sur ce point ni sur d'autres aspects du fonctionnement du système suédois.

344. En somme, aux fins de la présente étape de l'analyse, si la Cour a relevé au paragraphe précédent une lacune procédurale qu'il convient de combler, elle considère que, dans l'ensemble, les circonstances dans lesquelles les éléments interceptés doivent être détruits sont claires en droit suédois.

8) La supervision

345. En vertu du droit suédois, la tâche de supervision des activités de renseignement extérieur en général et de ROEM en particulier est confiée principalement à l'Inspection du renseignement extérieur. D'autres fonctions de supervision sont exercées par l'autorité de protection des données, qui dispose toutefois de moins de pouvoirs.

346. Observant que le conseil de l'Inspection est présidé par des juges permanents ou d'anciens juges et que ses membres, nommés par le gouvernement pour un mandat d'au moins quatre ans, sont choisis parmi des candidats proposés par les groupes parlementaires, la Cour estime établi que le rôle de l'Inspection est celui d'un mécanisme de contrôle indépendant.

347. L'Inspection dispose de pouvoirs étendus qui portent sur le déroulement des opérations de ROEM du début à la fin. Elle est en particulier chargée de donner au FRA l'accès aux canaux de transmission après avoir vérifié que l'accès demandé correspond à l'autorisation délivrée par le tribunal pour le renseignement extérieur (chapitre 6, article 19a de la loi sur les communications électroniques). Elle contrôle tous les autres aspects des activités du FRA, notamment l'interception, l'analyse, l'utilisation et la destruction des éléments recueillis. Il est important de noter qu'elle peut examiner les sélecteurs utilisés (article 10 de la loi relative au renseignement d'origine électromagnétique) et qu'elle a accès à tous les documents pertinents du FRA (paragraphes 50-53 ci-dessus).

348. Il apparaît donc que l'Inspection a les pouvoirs et les outils nécessaires non seulement pour vérifier le respect des exigences formelles du droit suédois, mais aussi pour examiner les aspects relatifs à la proportionnalité de l'atteinte aux droits individuels qui peut être occasionnée par les activités de ROEM. Il convient de relever à cet égard qu'au cours de ses inspections elle a procédé à de nombreuses vérifications détaillées, notamment quant aux sélecteurs employés (paragraphe 53 ci-dessus).

349. La requérante a souligné que certains des actes adoptés par l'Inspection revêtent la forme d'avis et de recommandations, plutôt que de décisions juridiquement contraignantes. Elle semble considérer que cela affaiblit considérablement l'impact réel du travail de l'Inspection.

350. La Cour observe qu'en vertu de l'article 10 de la loi relative au renseignement d'origine électromagnétique, l'Inspection peut, si elle constate que des signaux ont été indûment interceptés, ordonner par une décision juridiquement contraignante qu'il soit mis un terme à la collecte ou que les enregistrements ou notes concernant les données recueillies soient détruits. Sur certaines autres questions, telles que l'engagement potentiel de la responsabilité civile de l'État à l'égard d'une personne ou d'une organisation donnée, ou lorsque des éléments indiquent qu'une infraction pénale a peut-être été commise, l'Inspection est tenue de signaler les faits aux autorités compétentes pour prendre des décisions juridiquement contraignantes. La Cour juge ce dispositif satisfaisant. Elle observe que, s'il est vrai qu'il semble n'exister en droit suédois aucune possibilité juridique d'obtenir l'exécution des recommandations par lesquelles l'Inspection demande une évolution ou une rectification des pratiques du FRA, la Direction nationale du contrôle de la gestion publique, qui a vérifié les activités de supervision de l'Inspection en 2015, a constaté que le FRA disposait de procédures de prise en compte des avis rendus par l'Inspection et que les suggestions émises par celle-ci avaient été traitées avec sérieux et, si nécessaire, avaient donné lieu à des réformes. À l'exception d'un cas où il a déféré la question au gouvernement, le FRA a toujours pris les mesures demandées par l'Inspection (paragraphe 54 ci-dessus).

351. Par ailleurs, les informations dont dispose la Cour quant aux inspections menées par l'Inspection confirment que celle-ci contrôle activement les activités du FRA, non seulement en théorie mais aussi en pratique, sur un plan tant général et systématique que thématique. Ainsi, sur une période de huit ans, l'Inspection a réalisé 102 inspections, au cours desquelles elle a procédé à des vérifications détaillées des sélecteurs employés, de la destruction des renseignements, de la communication des rapports, de la coopération avec d'autres États et avec des organisations internationales, du traitement des données à caractère personnel et du respect général de la législation, des directives et des autorisations relatives aux activités de ROEM. Ces inspections ont donné lieu à plusieurs avis et suggestions adressés au FRA et à un avis remis au gouvernement. L'utilité de l'activité de l'Inspection est illustrée par le fait, par exemple, que lorsque, en 2011, celle-ci a invité le FRA à modifier ses règles internes concernant la destruction des données, la modification a été faite avant la fin de l'année (paragraphe 53 ci-dessus).

352. Enfin, l'Inspection rend des rapports annuels qui sont publics, et ses activités ont été contrôlées à plusieurs reprises par la Direction nationale du contrôle de la gestion publique (paragraphes 53 et 54 ci-dessus).

353. Dans ces conditions, il n'y a pas de raison de douter que le droit et la pratique nationaux garantissent une supervision effective des activités de ROEM en Suède. De l'avis de la Cour, le rôle de l'Inspection, d'une part, et la procédure judiciaire d'autorisation préalable par le tribunal pour le

renseignement extérieur, d'autre part, constituent ensemble une garantie efficace contre les abus aux stades essentiels du processus de ROEM : avant et pendant l'interception, l'analyse, l'utilisation et la destruction des informations obtenues.

9) Le contrôle a posteriori

354. Il apparaît qu'il n'est pas contesté qu'en raison du secret, il n'a jamais été fait usage en pratique de la possibilité offerte en théorie par la loi relative au renseignement d'origine électromagnétique d'aviser les personnes physiques concernées lorsque des sélecteurs les visant directement ont été employés (paragraphes 58, 59, 75 *in fine* et 80 ci-dessus).

355. De l'avis de la Cour, il est clair que, à supposer qu'elle soit techniquement possible, la notification aux personnes concernées d'activités menées dans le contexte du système suédois de ROEM aux fins du renseignement extérieur pourrait avoir des conséquences qui seraient d'une portée considérable et qu'il est difficile de prévoir à l'avance. Comme cela a déjà été observé (paragraphe 272 ci-dessus), un recours ne dépendant pas de la notification à la personne qui a fait l'objet de l'interception pourrait constituer un recours effectif dans le contexte de l'interception en masse. La Cour admet donc que l'approche de l'État défendeur à cet égard est légitime. Cependant, l'absence d'un mécanisme de notification efficace devrait être contrebalancée par des recours effectifs, ouverts à toute personne pensant que ses communications ont été interceptées et analysées.

356. La Cour note à cet égard que la loi relative au renseignement d'origine électromagnétique permet aux personnes physiques ou morales qui le souhaitent d'obtenir un contrôle *a posteriori* sans avoir à démontrer qu'elles ont probablement été concernées par une opération d'interception en masse. Toute personne, quels que soient sa nationalité et son lieu de résidence, peut saisir l'Inspection du renseignement extérieur. Celle-ci doit alors rechercher si les communications de cette personne ont été interceptées dans le cadre d'activités de ROEM et, si tel a été le cas, vérifier si l'interception et le traitement des informations correspondantes ont été effectués dans le respect du droit applicable. Comme cela a déjà été mentionné (paragraphe 350 ci-dessus), l'Inspection peut décider de mettre fin à une opération de ROEM ou ordonner la destruction des renseignements recueillis.

357. Selon la requérante, il est impossible pour un particulier de savoir si ses communications ont réellement été interceptées et, de manière générale, d'obtenir une décision motivée. En vertu du droit interne pertinent, l'Inspection informe simplement la personne qui l'a saisie qu'elle a procédé au contrôle sollicité (paragraphe 61 ci-dessus).

358. Il ressort des éléments dont dispose la Cour (voir, en particulier, les paragraphes 61 et 203 ci-dessus) que l'Inspection examine régulièrement les demandes dont la saisissent des particuliers.

359. La Cour observe cependant que, même s'il est vrai que l'Inspection est un organe indépendant, elle a notamment pour mission de superviser et de contrôler les activités du FRA et, dans ce cadre, de prendre ou d'approuver des décisions opérationnelles concernant pour certaines l'accès aux canaux de transmission, l'utilisation de sélecteurs, ainsi que l'analyse, l'utilisation et la destruction des éléments interceptés (paragraphes 50-53 ci-dessus). Ainsi, lorsque l'Inspection est amenée à exercer son rôle supplémentaire de contrôle *a posteriori* à la demande d'un particulier, elle peut se trouver dans une situation où il lui incombe de contrôler ses propres activités de supervision des mesures d'interception en masse mises en œuvre par le FRA. Compte tenu du secret qui entoure, légitimement, les procédures pertinentes, et en l'absence d'obligation juridique imposant à l'Inspection de rendre à la personne concernée une décision motivée, des doutes peuvent surgir sur le point de savoir si l'examen qu'elle fait des demandes dont elle est saisie en pareil cas offre des garanties adéquates d'objectivité et de minutie. On ne peut exclure que ce double rôle de l'Inspection risque de générer des conflits d'intérêts et, par conséquent, la tentation de passer sous silence une omission ou une faute afin d'éviter les critiques ou d'autres conséquences.

360. La Cour ne méconnaît pas, à cet égard, le fait que l'Inspection est elle-même soumise à des audits (paragraphe 54 ci-dessus), qui pourraient en principe être considérés comme une garantie pertinente. Elle constate cependant que le Gouvernement n'a fourni aucune information démontrant que les audits menés jusqu'à présent aient porté sur les contrôles effectués par l'Inspection à la demande d'une personne cherchant à savoir si ses communications avaient été interceptées par le FRA. Il apparaît que la Direction nationale du contrôle de la gestion publique – qui est chargée de vérifier un nombre important d'organes administratifs dans différents secteurs – n'est nullement tenue d'effectuer des vérifications aussi spécifiques et de le faire régulièrement. Dans ces conditions, et compte tenu du problème structurel relevé au paragraphe précédent, la Cour n'est pas convaincue que la simple possibilité pour la Direction nationale du contrôle de la gestion publique d'examiner le traitement fait par l'Inspection des demandes dont elle est saisie soit suffisante.

361. Par ailleurs, la Cour considère qu'un système de contrôle *a posteriori* dans lequel l'autorité saisie ne rend pas des décisions motivées communiquées aux intéressés, ou au moins des décisions contenant une motivation accessible à un avocat spécial titulaire d'une habilitation de sécurité, dépend trop largement de l'initiative et de la persévérance de fonctionnaires opérant à l'abri des regards. Elle observe que dans le système suédois, aucun détail n'est communiqué au demandeur quant à la teneur et à

l'issue du contrôle effectué par l'Inspection, laquelle semble ainsi bénéficier d'une grande latitude. Une décision motivée présente l'avantage indéniable de mettre à la disposition du public des indications quant à l'interprétation des règles juridiques applicables, aux limites à respecter et à la manière dont l'intérêt public et les droits individuels doivent être mis en balance dans le contexte spécifique de l'interception en masse de communications. Comme la Cour l'a noté dans l'arrêt *Kennedy* (précité, § 167), la publication de telles conclusions juridiques accroît le degré de contrôle exercé en la matière. Ces observations amènent la Cour à considérer que les caractéristiques susmentionnées du système suédois n'offrent pas une base suffisante pour que le public soit assuré que, si des abus devaient se produire, ils seraient dévoilés et réparés.

362. Il est vrai que les particuliers peuvent saisir les médiateurs parlementaires et le chancelier de la Justice et que ceux-ci peuvent examiner la conduite des autorités afin, notamment, d'en contrôler la légalité et de s'assurer qu'il n'a pas été porté atteinte à des droits et libertés fondamentaux. Le chancelier et les médiateurs peuvent engager des procédures pénales ou disciplinaires (paragraphes 66-68 ci-dessus). S'il s'agit là de mécanismes de plainte pertinents, la Cour observe qu'ils semblent ne pas avoir été utilisés fréquemment dans le contexte de l'interception en masse de communications (paragraphe 67 *in fine* ci-dessus). En tout état de cause, elle estime qu'une procédure juridique menée devant un organe indépendant qui, dans la mesure du possible, examine l'affaire de manière contradictoire et rende des décisions motivées et juridiquement contraignantes est un élément essentiel de l'effectivité d'un contrôle *a posteriori*. Or ni la plainte au chancelier ni la plainte aux médiateurs ne répondent à ces conditions.

363. Enfin, la Cour souscrit à l'argument de la requérante selon lequel le recours ouvert devant l'IPT au Royaume-Uni (*Big Brother Watch et autres*, précité, §§ 413-415) montre qu'il est possible de concilier les impératifs légitimes de sécurité et la nécessité d'assurer un contrôle *a posteriori* fiable des activités d'interception en masse.

364. En bref, le double rôle de l'Inspection et l'impossibilité pour les particuliers d'obtenir des décisions motivées sous quelque forme que ce soit en réponse à leurs plaintes ou questionnements concernant l'interception en masse de communications – éléments qui sont l'un et l'autre contraires aux exigences d'un contrôle *a posteriori* effectif – doivent être considérés comme une carence du régime suédois, dont il faut tenir compte pour apprécier la compatibilité de ce régime avec l'article 8 de la Convention. Compte tenu du fait qu'elle ne dispose d'informations suffisantes ni quant à la pratique du tribunal pour le renseignement extérieur relativement à l'autorisation judiciaire préalable de catégories de sélecteurs ou de sélecteurs forts (paragraphe 300 ci-dessus) ni quant à la manière dont les normes relatives à la destruction des éléments interceptés sont appliquées

dans la pratique (paragraphe 343 ci-dessus), la Cour juge cette carence particulièrement significative. Les éléments susmentionnés exacerbent indubitablement les craintes des individus concernés quant au point de savoir s'ils ont pu faire l'objet d'agissements arbitraires abusifs.

10) Conclusion

365. Il ne fait aucun doute pour la Cour que l'interception en masse est d'une importance vitale pour les États contractants, qui en ont besoin pour détecter les menaces pesant sur leur sécurité nationale. Cela a en particulier été reconnu par la Commission de Venise (paragraphe 86 ci-dessus). Il apparaît que, dans les conditions actuelles, aucune autre solution ou combinaison de solutions ne serait suffisante pour remplacer cette activité.

366. La Cour rappelle par ailleurs qu'elle n'a pas pour tâche de prescrire un modèle idéal pour le ROEM mais de contrôler la conformité à la Convention des dispositifs juridiques et pratiques existants, lesquels varient dans leur conception et dans leur fonctionnement d'une Partie contractante à l'autre. Elle doit pour ce faire considérer comme un tout le modèle de ROEM – en l'espèce le modèle suédois – et ses garanties contre les abus.

367. Dans le cas présent, l'examen du système suédois d'interception en masse a révélé que celui-ci est fondé sur des règles juridiques détaillées, que sa portée est clairement délimitée et qu'il offre des garanties. Les motifs pour lesquels l'interception en masse peut être autorisée en Suède sont clairement définis, les circonstances dans lesquelles les communications peuvent être interceptées et examinées sont énoncées avec une clarté suffisante, la durée de l'interception est juridiquement encadrée et contrôlée, et les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés sont assorties de garanties adéquates contre les abus. Les mêmes protections s'appliquent au contenu des communications interceptées et aux données de communication.

368. Surtout, la procédure judiciaire d'autorisation préalable telle qu'elle existe en Suède et la supervision exercée par un organe indépendant permettent en principe de garantir en pratique l'application des règles du droit interne et des standards de la Convention et de limiter le risque de conséquences disproportionnées portant atteinte aux droits protégés par l'article 8. Il convient notamment de tenir compte du fait qu'en Suède, les limites à respecter pour chaque mission d'interception en masse ainsi que la légalité et la proportionnalité de la mission font l'objet d'une procédure judiciaire d'autorisation préalable devant le tribunal pour le renseignement extérieur, qui siège en présence d'un représentant chargé de la protection de la vie privée défendant l'intérêt public.

369. La Cour a constaté trois carences dans le régime suédois d'interception en masse : l'absence de règle claire concernant la destruction des éléments interceptés qui ne contiennent pas de données à caractère personnel (paragraphe 342 ci-dessus), le fait que ni la loi relative au

renseignement d'origine électromagnétique ni aucun autre texte n'énonce l'obligation de prendre en compte les intérêts liés à la vie privée lorsqu'une décision de partage de renseignements avec des partenaires étrangers est adoptée (paragraphes 326-330 ci-dessus) et l'absence de contrôle *a posteriori* effectif (paragraphes 359-364 ci-dessus).

370. Le potentiel de conséquences négatives sur l'exercice des droits protégés par l'article 8 qui découle de la première de ces carences est limité par le fait que le droit suédois renferme des règles claires prévoyant la destruction des éléments interceptés dans un certain nombre de circonstances et, en particulier, lorsqu'ils contiennent des données à caractère personnel.

371. La Cour considère en revanche que la deuxième carence pourrait entraîner des conséquences négatives très importantes pour les personnes physiques ou morales concernées. Comme elle l'a relevé, cette carence pourrait en effet permettre la transmission mécanique vers l'étranger d'informations, dont la communication porte gravement atteinte au droit au respect de la vie privée ou au droit au respect de la correspondance, qui ne présenteraient pourtant que très peu d'intérêt pour le renseignement. Une telle transmission peut ainsi engendrer des risques manifestement disproportionnés d'atteinte aux droits protégés par l'article 8 de la Convention. Par ailleurs, aucune obligation juridiquement contraignante n'impose au FRA d'analyser les garanties offertes par le destinataire étranger des renseignements afin de déterminer si elles sont d'un niveau minimum acceptable.

372. Enfin, le double rôle de l'Inspection et l'impossibilité pour les particuliers d'obtenir des décisions motivées sous quelque forme que ce soit en réponse à leurs plaintes ou interrogations concernant l'interception en masse de communications affaiblissent le mécanisme de contrôle *a posteriori* dans une mesure qui engendre des risques pour le respect des droits fondamentaux des personnes concernées. Par ailleurs, l'absence de contrôle effectif au dernier stade de l'interception n'est pas conciliable avec la situation constatée par la Cour, où l'intensité de l'ingérence faite dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance (paragraphes 239 et 245 ci-dessus), et elle ne satisfait pas à l'exigence de « garanties de bout en bout » (paragraphe 264 ci-dessus).

373. La Cour est convaincue que les caractéristiques principales du régime suédois d'interception en masse répondent aux exigences de la Convention relatives à la qualité de la loi, et elle considère que tel qu'il fonctionnait au moment où la chambre l'a examiné, ce régime demeurait dans la plupart de ses aspects dans les limites de ce qui est « nécessaire dans une société démocratique ». Elle juge en revanche que les carences mentionnées aux paragraphes précédents ne sont pas suffisamment compensées par les garanties existantes et que, partant, le régime suédois

d'interception en masse excède la marge d'appréciation accordée aux autorités de l'État défendeur à cet égard. Elle 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 261 ci-dessus). Eu égard au principe de la prééminence du droit, laquelle est expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8 (*Roman Zakharov*, précité, § 228), la Cour estime donc que le régime suédois d'interception en masse, considéré dans son ensemble, ne contient pas de « garanties de bout en bout » suffisantes pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus.

d) Conclusion sur l'article 8

374. Eu égard à la conclusion à laquelle elle est parvenue ci-dessus quant à la légalité et au caractère justifié du régime d'interception en masse contesté, la Cour conclut qu'en l'espèce il y a eu violation de l'article 8 de la Convention.

III. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 13 DE LA CONVENTION

375. La requérante allègue que les recours disponibles dans le régime suédois d'interception en masse sont insuffisants et ne répondent pas aux exigences de l'article 13 de la Convention. Cette disposition est libellée comme suit :

> « Toute personne dont les droits et libertés reconnus dans la (...) Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

376. La chambre a estimé qu'aucune question distincte ne se posait sur le terrain de cette disposition (paragraphe 184 de l'arrêt de la chambre).

377. La Grande Chambre adopte la même conclusion, compte tenu du constat de violation de l'article 8 auquel elle est parvenue ci-dessus.

IV. SUR L'APPLICATION DE L'ARTICLE 41 DE LA CONVENTION

378. 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

379. La requérante estime qu'un constat de violation constituerait en soi une réparation suffisante. Le Gouvernement est du même avis.

380. Dès lors, la Cour n'alloue aucune somme à ce titre.

B. Frais et dépens

381. La requérante demande 544 734 couronnes suédoises (SEK) pour 217 heures de travail juridique aux fins de la procédure devant la chambre et 190 heures de travail juridique aux fins de la procédure devant la Grande Chambre (soit 407 heures au total), à un taux horaire variant de 1 302 à 1 380 SEK.

382. La requérante demande également le remboursement des frais de déplacement et d'hébergement engagés pour la participation de ses trois représentants à l'audience tenue le 10 juillet 2019 devant la Grande Chambre. Ces frais s'élèvent à 8 669 SEK pour les billets d'avion et 8 231 SEK pour l'hébergement hôtelier (16 900 SEK au total). La requérante produit des copies des factures pertinentes.

383. Le montant total demandé par la requérante s'élève ainsi à 561 634 SEK (l'équivalent d'environ 52 625 EUR).

384. Le Gouvernement ne s'oppose pas aux sommes demandées par la requérante mais plaide que si la Cour ne conclut à la violation que de l'un des articles de la Convention invoqués, il y aura lieu de réduire le remboursement en conséquence.

385. 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 exposés ci-dessus, et étant donné qu'elle a constaté une violation de la Convention relativement au grief principal de la requérante, à savoir celui formulé sur le terrain de l'article 8, la Cour estime raisonnable la somme de 52 625 EUR tous frais et dépens confondus et l'accorde à la requérante.

C. Intérêts moratoires

386. 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. *Rejette*, à l'unanimité, l'exception préliminaire soulevée par le gouvernement défendeur relativement à la qualité de victime de la requérante ;

2. *Dit*, par quinze voix contre deux, qu'il y a eu violation de l'article 8 de la Convention ;

3. *Dit*, à l'unanimité, qu'il n'y a pas lieu d'examiner séparément le grief fondé sur l'article 13 de la Convention ;

4. *Dit*, à l'unanimité,
   a) que l'État défendeur doit verser à la requérante pour frais et dépens, dans les trois mois, la somme de 52 625 EUR plus tout montant pouvant être dû par l'intéressée à titre d'impôt, à convertir dans la monnaie de l'État défendeur au taux applicable à la date du règlement ;
   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 ;

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 de la Cour.

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 concordante commune des juges Lemmens, Vehabović et Bošnjak ;
– opinion concordante du juge Pinto de Albuquerque ;
– déclaration de vote commune aux juges Kjølbro et Wennerström.

R.S.O.
S.C.P.

OPINION CONCORDANTE COMMUNE AUX JUGES LEMMENS, VEHABOVIĆ ET BOŠNJAK

(Traduction)

Dans la présente affaire, nous avons voté avec la majorité sur tous les points du dispositif. Comme dans l'affaire connexe *Big Brother Watch et autres c. Royaume-Uni* (n^{os} 58170/13, 62322/14 et 24969/15), nous considérons toutefois que cet arrêt aurait dû aller bien plus loin dans la réaffirmation de l'importance de la protection de la vie privée et de la correspondance, en particulier en introduisant des garanties minimales plus strictes, mais aussi en appliquant ces garanties de manière plus rigoureuse au régime d'interception en masse litigieux. Les arguments que nous avons développés dans notre opinion concordante jointe à l'arrêt *Big Brother Watch et autres* sont largement applicables au présent cas d'espèce. Afin d'éviter toute répétition inutile, nous renvoyons donc le lecteur à cette opinion séparée. Cependant, le cadre juridique applicable aux deux régimes d'interception en masse examinés présentant des différences, certains passages de ladite opinion ne sont pas pertinents relativement à la présente affaire : nous invitons le lecteur à simplement les ignorer.

OPINION CONCORDANTE DU JUGE PINTO DE ALBUQUERQUE

(Traduction)

1. J'ai voté avec la majorité mais pour des raisons très différentes. Le cadre juridique suédois qui régit l'interception en masse est problématique sous de nombreux aspects que la majorité a ignorés ou minimisés. La pratique nationale est même pire. Elle est en effet très opaque, plus même que celle du Royaume-Uni. La Cour européenne des droits de l'homme (« la Cour ») a pourtant choisi de trancher la présente affaire sans avoir connaissance de certaines caractéristiques importantes de cette pratique, notamment concernant la manière dont les journaux d'historique et les archives sont réellement tenus à chaque étape des opérations d'interception en masse. Le Gouvernement a curieusement été dispensé d'apporter des éléments de preuve à l'appui de ses allégations parce que la Cour en a tout simplement présumé la véracité[1]. Plus déconcertant encore, la Cour n'a même pas eu accès à la jurisprudence pertinente de la juridiction nationale compétente en matière d'interception en masse, ignorant ainsi, par exemple, la véritable interprétation donnée par le tribunal pour le renseignement extérieur à l'article 3 de la loi relative au renseignement d'origine électromagnétique[2]. Tout comme dans l'affaire *Big Brother Watch et autres* (n^{os} 58170/13, 62322/14 et 24960/15), la méthodologie biaisée suivie par la Cour et le langage vague qu'elle emploie conduisent à un régime de garanties déficient en l'espèce[3].

I. LES BUTS DE L'INTERCEPTION EN MASSE TELS QU'ÉNONCÉS PAR LA LOI

2. L'imprévisibilité des buts poursuivis par l'interception en masse, tels qu'énoncés par la loi relative au renseignement d'origine électromagnétique, constitue la première des principales carences entachant le régime suédois. Les menaces militaires extérieures pesant sur le pays, dont il est question dans le premier de ces buts, « ne consistent pas

[1] Paragraphe 311 du présent arrêt : « il n'y a pas de raison de considérer qu'il n'est pas conservé en pratique des journaux d'historique et des archives détaillés ou que le FRA pourrait modifier arbitrairement ses instructions internes et supprimer ainsi son obligation à cet égard ». Le FRA se réfère à l'Institut national de la défense radio (*Försvarets radioanstalt*).

[2] Paragraphe 300 du présent arrêt : « Aucune explication n'a été produite devant la Cour quant à l'interprétation de [l'article 3 de la loi relative au renseignement d'origine électromagnétique] dans la pratique du tribunal pour le renseignement extérieur ». Je reviendrai plus loin sur ce point.

[3] Pour une critique du régime *pro autoritate* d'interception en masse admis par la Cour, je renvoie à mon opinion séparée jointe à l'arrêt *Big Brother Watch et autres*.

seulement en des menaces imminentes telles des menaces d'invasion, elles peuvent aussi englober des phénomènes susceptibles de se transformer, à long terme, en menaces pour la sécurité »[4]. Il s'agit d'une finalité très vague, tant dans sa dimension temporelle que spatiale, qui permet la surveillance d'étrangers, de minorités et d'entreprises légales qui pourraient être considérés comme des menaces potentielles à long terme.

3. Le but de la collecte d'informations sur le contexte stratégique en matière de terrorisme international ou d'autres formes graves de criminalité transfrontière risquant de menacer des intérêts nationaux essentiels, notamment « le trafic de stupéfiants ou la traite d'êtres humains, susceptibles par leur échelle de menacer d'importants intérêts nationaux »[5] ne définit pas suffisamment ce qu'est une forme grave de criminalité transfrontière. En droit international, la notion d'infraction grave englobe les infractions passibles d'une peine privative de liberté d'une durée de quatre ans ou plus[6]. Pour être prévisible, la notion de formes graves de criminalité susceptibles de déclencher une interception en masse devrait donc se rapporter à une liste précise d'infractions graves ou, de manière générale, à des infractions passibles d'une peine de quatre ans ou plus d'emprisonnement. Tel n'est pas le cas en Suède.

4. Le but de recueillir des informations sur le développement et la prolifération d'armes de destruction massive, d'équipements militaires ou d'autres produits similaires déterminés peut englober, « notamment, les activités pertinentes dans le cadre des engagements de la Suède en matière de non-prolifération et de contrôle des exportations, même si elles ne constituent pas une infraction et ne contreviennent à aucune convention internationale »[7]. Selon les informations officiellement fournies par le Gouvernement[8], les « autres produits similaires déterminés » comprennent les munitions et les produits à double usage, militaire et civil, et même l'assistance technique au sens de la loi sur le contrôle des produits à double usage et de l'assistance technique (2000: 1064). Les activités surveillées (« notamment ») ne sont toutefois pas suffisamment définies. L'espionnage économique et commercial au bénéfice de l'armement, de l'aérospatiale, de l'électronique, de la pétrochimie et d'autres industries manufacturières de la Suède sont-ils inclus dans ce but ?

---

[4] Paragraphe 23 du présent arrêt.
[5] *Ibidem*.
[6] Selon l'article 2 b) de la Convention des Nations unies contre la criminalité transnationale organisée, 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. Le rapport explicatif de la Recommandation Rec(2005)10 du Comité des Ministres du Conseil de l'Europe suit cette approche (paragraphe 20 du rapport explicatif).
[7] Paragraphe 23 du présent arrêt.
[8] https://www.loc.gov/law/help/foreign-intelligence-gathering/sweden.php#Signal

5. Le but de recueillir des informations sur des risques extérieurs menaçant gravement l'infrastructure sociale « inclut, notamment, les menaces informatiques graves provenant de l'étranger. Par menaces graves, on entend celles qui, par exemple, sont dirigées contre des structures publiques essentielles pour l'approvisionnement en énergie et en eau, pour la communication ou pour les services monétaires »[9]. Ni le type de menaces (« notamment ») ni les infrastructures publiques qui pourraient être menacées (« par exemple ») ne sont suffisamment circonscrits. Cet objectif signifie-t-il, par exemple, qu'une grève générale dans un pays voisin qui pourrait en fin de compte perturber et déstabiliser le système suédois de distribution d'énergie ou de pétrole pourrait justifier la surveillance des syndicats et de leurs membres qui ont participé à la grève ? Que se passe-t-il si la « menace » présumée est dirigée contre le système de transports publics ou les infrastructures sportives de la Suède ? Un déplacement massif de supporters étrangers pour un championnat de football en Suède justifie-t-il la surveillance de tous les supporters de football provenant des pays participant au championnat ?

6. Le but de la collecte d'informations sur les actes ou les intentions d'une puissance étrangère qui revêtent une importance particulière pour la politique étrangère, la politique de défense ou la politique de sécurité de la Suède est formulé en des termes très généraux. Il est précisé qu'« il ne suffit pas que le phénomène soit d'intérêt général mais qu'il faut que les renseignements aient un impact direct sur les actes ou les positions de la Suède dans différents domaines de la politique étrangère, de la politique de sécurité ou de la politique de défense »[10], mais cette précision est insuffisante puisqu'elle ne circonscrit ni le seuil de pertinence ni les domaines particuliers en jeu. Il est également préoccupant que de simples « intentions » d'une puissance étrangère puissent justifier le lancement d'une opération de surveillance, puisque cela laisse la porte ouverte à un contrôle des *Weltanschauungen* philosophiques et religieuses « étranges ». La surveillance des « causes »[11] des conflits ethniques, religieux et politiques, qui est comprise dans le but de recueillir des renseignements sur des conflits à l'étranger susceptibles d'avoir des répercussions sur la sécurité internationale, relève de cette même politique orwellienne du contrôle de la pensée remise au goût du jour[12].

---

[9] Paragraphe 23 du présent arrêt.

[10] *Ibidem*.

[11] *Ibidem*.

[12] De même, dans ses Observations finales concernant le septième rapport périodique de la Suède (28 avril 2016, CCPR/C/SWE/CO/7, § 36), le Comité des droits de l'homme des Nations unies s'est déclaré « préoccupé par le degré limité de transparence quant à la portée de ces pouvoirs de surveillance et aux garanties concernant leur application ». Je voudrais souligner que, dans son rapport du 22 février 2016 (A/HRC/31/65, § 43), le Rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a considéré que « pour mettre au point des

7. Le but poursuivi par les « activités de développement »[13] est un véritable trou noir juridique qui permet d'intercepter et d'analyser des communications qui ne relèvent d'aucun des huit buts du renseignement extérieur[14]. Il s'agit d'un chèque en blanc accordé aux autorités afin qu'elles puissent surveiller « de très larges segments du trafic international de signaux »[15]. L'argument du Gouvernement selon lequel ces données ne donnent lieu à aucun rapport de renseignement mais sont essentielles pour surveiller « les modifications constantes de l'environnement électromagnétique, des progrès techniques et de la protection des signaux »[16] revient à dire que toutes les communications sur Internet devraient être examinées afin que le FRA puisse suivre le rythme de l'évolution constante de l'environnement Internet, des progrès techniques et de la protection d'Internet. C'est évidemment absurde mais c'est en pratique ce qu'affirme le Gouvernement. La collecte sans but (c'est-à-dire hors des huit buts énoncés par la loi) d'un volume aussi illimité de données représente en soi une ingérence disproportionnée au sens des articles 8 et 10 de la Convention européenne des droits de l'homme (« la Convention »).

8. Enfin, il est également préoccupant que les pouvoirs de plus en plus importants dont disposent les services répressifs (tels que la Sûreté et la direction des opérations nationales de l'autorité de police) pour obtenir des renseignements d'origine électromagnétique et accéder aux données recueillies, ou aux rapports de renseignement, soulèvent des doutes quant au respect du principe de finalité qui sous-tend le régime suédois d'interception en masse, en vertu duquel les données ne peuvent être collectées et traitées qu'à des fins spécifiques énoncées par la loi et ne peuvent être utilisées d'une manière incompatible avec ces finalités, par exemple dans un but de répression dans le cadre de poursuites pénales. En effet, l'Inspection du renseignement extérieur elle-même a récemment alerté sur le fait que les services répressifs ne seraient pas en mesure de conserver les informations reçues du FRA séparément de leurs activités de répression[17].

---

stratégies efficaces, les États ne devraient pas se fonder sur des idées préconçues ou fausses concernant les groupes qui seraient les plus susceptibles de basculer dans la radicalisation ou dans l'extrémisme violent, mais s'appuyer sur des données afin de bien comprendre les problèmes nationaux et locaux qui influent sur le processus de radicalisation ».

[13] Paragraphe 24 du présent arrêt.

[14] Comme l'a conclu dans son rapport le comité sur le renseignement d'origine électromagnétique (paragraphe 79 du présent arrêt).

[15] Paragraphe 292 du présent arrêt.

[16] Plaidoiries du Gouvernement lors de l'audience devant la Grande Chambre le 10 juillet 2019.

[17] Voir la référence à l'avis de l'Inspection du renseignement extérieur dans les observations produites par la requérante devant la Grande Chambre le 3 mai 2019, p. 24. Cet avis n'a pas été contesté par le Gouvernement.

II. L'AUTORISATION DE L'INTERCEPTION EN MASSE

9. La législation suédoise confie la procédure d'autorisation des mesures de surveillance en masse à un tribunal. Mais le tribunal pour le renseignement extérieur n'est pas une juridiction ordinaire. Et c'est là que réside la deuxième carence principale du régime suédois. Le tribunal pour le renseignement extérieur est composé d'un président, d'un ou deux vice-présidents et de deux à six juges non professionnels, essentiellement d'anciens hommes politiques[18], tous nommés par le gouvernement pour un mandat de quatre ans. Leur nomination est renouvelable, ce qui renforce leur lien politique avec le gouvernement. Même le représentant chargé de la protection de la vie privée, qui est supposé défendre l'intérêt public et non pas représenter la personne concernée par une mesure de renseignement, est nommé par le gouvernement pour un mandat renouvelable, et il est possible de se passer de son intervention. Si l'urgence de l'affaire est telle qu'un retard compromettrait gravement la réalisation du but de la demande, le tribunal peut siéger et prendre une décision sans que ledit représentant ne soit présent ni n'ait la possibilité de produire des observations d'une autre manière. Le statut hautement politisé des membres du tribunal pour le renseignement extérieur cadre avec le fait que celui-ci n'ait jamais tenu d'audience publique et que ses décisions soient définitives et confidentielles[19]. Au vu de ces caractéristiques, le tribunal pour le renseignement extérieur se rapproche davantage d'un organe politique que d'un organe judiciaire véritablement indépendant[20].

10. Le contrôle exercé par le tribunal pour le renseignement extérieur porte sur les « canaux de transmission » auxquels le FRA demande à avoir

---

[18] Voir le rapport de la Commission de Venise sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique, 2015, p. 39.

[19] Je ne parviens pas à comprendre pourquoi la majorité reproche à l'Inspection du renseignement extérieur (qui n'est pas une juridiction) de ne pas rendre de décisions publiques mais est disposée à accepter que le tribunal pour le renseignement extérieur (qui est une juridiction) ne rende pas de décisions publiques (comparer les paragraphes 297 et 372 du présent arrêt).

[20] La Commission de Venise l'a qualifié d'« organe hybride » (rapport de la Commission de Venise, précité, p. 39). C'est pourquoi le Comité des droits de l'homme des Nations unies a demandé à l'État suédois de s'assurer que « des mécanismes de surveillance indépendants et efficaces de l'échange de données personnelles soient mis en place » (Observations finales concernant le septième rapport périodique de la Suède, précité, § 37). Il ne s'agit pas d'un cas isolé en Europe. L'Agence des droits fondamentaux de l'Union européenne (« la FRA de l'UE ») a relevé les carences suivantes dans les États de l'Union européenne : « l'enquête a également révélé des limites à l'indépendance totale. Certains organes de contrôle demeurent fortement dépendants de l'exécutif : la loi ne leur confère pas de pouvoirs décisionnels contraignants, leur personnel et leur budget sont limités, ou leurs locaux sont situés dans des bâtiments gouvernementaux » (FRA de l'UE, Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'Union européenne, Volume II, Résumé, 2017, p. 9).

accès, ainsi que sur les « sélecteurs » (termes de recherche) et les catégories de sélecteurs qu'il entend utiliser pour la collecte automatisée de données, et sur la durée de l'autorisation de surveillance. Mais rien n'impose l'annulation de l'autorisation si la collecte de communications cesse d'être nécessaire[21] ou la destruction après un certain temps des éléments interceptés qui ne contiennent pas de données à caractère personnel[22]. De même, le tribunal pour le renseignement extérieur n'est pas tenu de s'assurer qu'un soupçon raisonnable pèse sur la personne ciblée. Il est vrai que les sélecteurs forts se rapportant directement à une personne physique donnée ne peuvent être utilisés que s'ils revêtent une « importance exceptionnelle » pour les activités de renseignement[23], mais cette restriction ne s'applique qu'aux sélecteurs employés dans le cadre de la collecte automatisée de données, et non à ceux utilisés pour effectuer une recherche plus approfondie dans les données collectées. Cela signifie que la loi accorde une importante latitude dans la collecte de communications et dans la recherche que le FRA effectue sur ces communications et les données de communication associées, en particulier lorsque l'autorisation octroyée par le tribunal pour le renseignement extérieur porte sur des catégories de sélecteurs[24]. Le problème du manque de spécificité des sélecteurs semble même plus sérieux concernant les sélecteurs employés pour les données de communication associées[25].

11. Par ailleurs, rien ne montre que le tribunal pour le renseignement extérieur peut apprécier, et apprécie effectivement, la nécessité de protéger les communications relevant du secret professionnel, notamment lorsqu'il

---

[21] La majorité néglige l'importance de cette carence, confondant « l'existence de mécanismes de supervision » avec une garantie spécifique sur le fond qui imposerait la cessation des mesures d'interception qui ne sont plus nécessaires (paragraphe 336 du présent arrêt).

[22] La majorité considère que, « dans l'ensemble », les règles relatives à la destruction des éléments interceptés qui contiennent des données à caractère personnel sont suffisamment claires, ignorant toutefois la lacune réglementaire concernant les éléments qui ne contiennent aucune donnée à caractère personnel (paragraphe 344 du présent arrêt).

[23] Je suis troublé par le fait que la majorité soit disposée à admettre que le critère de l'« importance exceptionnelle » pour l'autorisation de sélecteurs forts est « de nature à offrir une protection renforcée pertinente » alors qu'elle n'a aucune idée de la manière dont le tribunal pour le renseignement extérieur applique ce critère (paragraphe 300 du présent arrêt). Cela revient à donner un chèque en blanc au tribunal pour le renseignement extérieur et au gouvernement suédois.

[24] La majorité le reconnaît à juste titre, admettant qu'« il peut être difficile » d'apprécier la question de la proportionnalité lorsque la demande d'autorisation formulée par le FRA indique seulement des catégories de sélecteurs (paragraphe 301 du présent arrêt). C'est précisément la raison pour laquelle les interceptions en masse fondées sur des catégories de sélecteurs ne devraient pas être autorisées (voir mon opinion séparée jointe à l'arrêt *Big Brother Watch et autres*, précité).

[25] C'est ce qui a été conclu par le comité sur le renseignement d'origine électromagnétique dans son rapport (paragraphe 78 du présent arrêt) et admis par le Gouvernement (paragraphe 220 du présent arrêt).

existe une probabilité raisonnable que de telles communications soient accidentellement « prises dans les filets » de l'interception demandée. Les communications relevant du secret professionnel, telles que celles relatives aux sources journalistiques ou celles protégées par le principe de la confidentialité des échanges entre l'avocat et son client, ne sont protégées que dans la mesure où elles doivent être détruites si elles ont été interceptées. Il est plutôt troublant que même les communications dans le contexte religieux de la confession ou du conseil individuel ne soient pas protégées puisqu'elles peuvent être interceptées et, exceptionnellement, examinées.

III. LA SUPERVISION DE LA MISE EN ŒUVRE DE L'AUTORISATION D'INTERCEPTION

12. Le tribunal pour le renseignement extérieur ne contrôle ni la mise en œuvre de l'autorisation d'interception en masse ni même l'utilisation envisagée des communications interceptées, puisque cette tâche est confiée à l'Inspection du renseignement extérieur. Tout comme la composition du tribunal pour le renseignement extérieur, celle du conseil de l'Inspection dépend du gouvernement qui nomme ses membres pour un mandat de quatre ans renouvelable. Le président et le vice-président dudit conseil doivent être ou avoir été juges permanents. Les quatre autres membres sont choisis parmi d'anciens hommes politiques sur proposition des groupes parlementaires[26]. L'Inspection du renseignement extérieur travaille à temps partiel[27] et elle est assistée d'un « petit secrétariat »[28].

13. L'Inspection n'a pas le pouvoir de se prononcer, au moyen de décisions juridiquement contraignantes, sur la légalité de l'autorisation délivrée par le tribunal pour le renseignement extérieur, ni celui d'ordonner un changement dans la pratique du FRA ou la modification de son règlement intérieur, ni encore celui d'octroyer une réparation, mais elle peut décider de la cessation d'une opération d'interception ou de la destruction des éléments interceptés si ladite opération n'a pas respecté l'autorisation sur laquelle elle était fondée. L'Inspection ne peut prendre aucune décision juridiquement contraignante relativement à des violations de la Convention, de la Constitution suédoise ou de la loi sur le traitement des données à caractère personnel dans le cadre des activités du FRA. Si elle constate une telle violation, elle ne peut que remettre un rapport à l'autorité de protection des données.

---

[26] La Commission de Venise a qualifié l'Inspection du renseignement extérieur d'« organe hybride », comme elle l'a fait pour le tribunal pour le renseignement extérieur (rapport de la Commission de Venise, précité, p. 39).

[27] Comme l'a admis le Gouvernement lors de l'audience devant la Grande Chambre le 10 juillet 2019.

[28] Comme l'a décrit la Commission de Venise dans son rapport précité, p. 39.

14. L’autorité de protection des données exerce une fonction de supervision générale de la protection des données à caractère personnel. Dans l’exercice de cette fonction, elle peut accéder aux données à caractère personnel traitées par le FRA, aux documents relatifs au traitement de ces données, ainsi qu’aux lieux où celles-ci sont traitées. Elle ne peut prendre aucune décision juridiquement contraignante à l’égard du FRA et n’est nullement tenue de prendre des mesures après avoir reçu un rapport de l’Inspection. Si elle choisit d’agir, tout ce qu’elle peut faire est communiquer ses observations au FRA ou saisir le tribunal administratif pour obtenir la destruction des données à caractère personnel traitées de manière illégale. À ce jour, elle n’a toutefois jamais fait usage de cette faculté[29].

15. Enfin, en termes de contrôle interne, le conseil de protection de la vie privée du FRA, qui est chargé de contrôler les mesures prises pour garantir la protection de l’intégrité personnelle, est également composé de membres nommés par le gouvernement. Cet organe apparaît sans influence, comme le montre le fait qu’ en 2010 et en 2016 l’autorité de protection des données a reproché au FRA, sans succès, de ne pas contrôler suffisamment les journaux d’historique permettant de détecter l’utilisation injustifiée de données à caractère personnel[30]. L’introduction alléguée par le Gouvernement d’un groupe fonctionnel central en 2018 pour la surveillance et le suivi des journaux d’historique ne suffit pas. En effet, aucune obligation légale n’impose au FRA de tenir des journaux d’historique et des archives détaillées à chaque étape des opérations d’interception en masse, notamment aux stades de l’interception, de l’utilisation ultérieure et de la communication des données. Cela signifie que la pratique de tenue des archives du FRA, si elle existe, dépend des procédures internes et du pouvoir d’appréciation de cet organisme.

IV. LES RECOURS

16. L’absence d’un véritable mécanisme indépendant d’autorisation et de supervision de la mise en œuvre des mesures d’interception en masse est aggravée par le caractère purement virtuel des recours qui sont ouverts aux personnes ayant fait l’objet d’une mesure d’interception[31]. La loi prévoit que ces dernières doivent être avisées de l’interception dont elles ont fait

[29] Paragraphe 57 du présent arrêt.

[30] Paragraphe 76 du présent arrêt.

[31] L’Agence des droits fondamentaux de l’Union européenne a souligné que l’effectivité des voies de recours dépend de la capacité de l’organe compétent de prendre des décisions juridiquement contraignantes qui doivent, au minimum, inclure la possibilité d’ordonner la cessation de la surveillance, la destruction des données recueillies illégalement et le versement d’une réparation appropriée (FRA de l’UE, Surveillance par les services de renseignement, précité, 2017, p. 114 de la version anglaise du rapport).

l'objet lorsque des sélecteurs les visant directement ont été employés et que le secret ne s'y oppose pas. Cette garantie ne concerne que les personnes physiques, et non les personnes morales telles que la requérante. En tout état de cause, cette loi est restée lettre morte[32].

17. En outre, toute personne physique ou morale peut saisir l'Inspection du renseignement extérieur. Celle-ci doit alors vérifier si l'interception et le traitement des données interceptées ont été effectués dans le respect du droit applicable. Étonnamment, dans les 132 demandes qu'elle a traitées, l'Inspection ne s'est jamais prononcée en faveur du demandeur[33], pour la simple raison que l'Inspection est *iudex in causa sua* en ce qu'il lui est demandé de contrôler la supervision qu'elle a elle-même exercée, sans même devoir informer le plaignant de ses conclusions ou motiver ses décisions[34]. Les méthodes de travail de l'Inspection du renseignement extérieur ne sont pas si éloignées du procès sombre et ténébreux décrit par Franz Kafka.

18. Par ailleurs, les personnes concernées peuvent demander au FRA la divulgation et des mesures correctives concernant des données à caractère personnel qui ont été traitées, et les décisions du FRA à cet égard peuvent faire l'objet d'un recours devant le tribunal administratif. Toutefois, les règles nationales sur le secret peuvent faire obstacle au droit de la personne à accéder à ces informations[35] ainsi qu'au pouvoir du tribunal administratif de contrôler l'appréciation faite par le FRA de la nécessité d'appliquer les restrictions liées au secret. Cette impasse est mise en évidence par le fait que la possibilité de saisir le tribunal administratif n'a jamais été utilisée[36]. En

[32] Paragraphes 60 et 80 du présent arrêt. En effet, le Comité des droits de l'homme des Nations unies a demandé à l'État suédois de s'assurer que « les personnes concernées aient accès comme il convient à des voies de recours utiles en cas d'abus » (Observations finales concernant le septième rapport périodique de la Suède, précité, § 37).

[33] Paragraphe 61 du présent arrêt. Au paragraphe 218 du présent arrêt, il est fait référence à 141 contrôles effectués à la demande d'une personne, dont aucun d'entre eux n'a révélé d'« interception irrégulière ». Ce que la majorité cherche à démontrer à cet égard n'est pas clair. D'un côté, elle admet que les décisions puissent être notifiées à un « avocat spécial titulaire d'une habilitation de sécurité », mais de l'autre elle exige qu'elles soient « à la disposition du public » et critique « l'impossibilité pour les particuliers d'obtenir des décisions motivées sous quelque forme que ce soit en réponse à leurs plaintes » (comparer les paragraphes 361 et 372 du présent arrêt).

[34] On est bien loin de la norme de l'Union européenne telle qu'énoncée par l'Agence des droits fondamentaux de l'Union européenne (FRA de l'UE, Surveillance par les services de renseignement, précité, p. 12) : « Les États membres devraient veiller à ce que les organes juridictionnels et non juridictionnels ayant des pouvoirs de réparation aient la capacité et les compétences nécessaires pour évaluer les plaintes individuelles liées au renseignement et statuer efficacement sur celles-ci. (…) En particulier, l'organe chargé du traitement des recours devrait avoir accès aux locaux des services de renseignement et aux données recueillies, pouvoir prendre des décisions contraignantes, et informer les plaignants des conclusions de ses enquêtes. Les personnes concernées devraient pouvoir faire appel des décisions les concernant. »

[35] Comme la chambre elle-même l'a admis (§ 175 de l'arrêt de la chambre).

tout état de cause, cette voie de recours n'est pas ouverte aux personnes morales telles que la requérante.

19. Enfin, ni les médiateurs parlementaires ni le chancelier de la Justice n'exercent un contrôle efficace puisqu'ils ne peuvent adopter de décisions juridiquement contraignantes ordonnant la cessation d'une opération d'interception ou la destruction des éléments interceptés. De fait, aucun d'entre eux n'a jamais jugé nécessaire d'agir dans le cadre de ses compétences en la matière, par exemple en engageant des procédures pénales ou disciplinaires contre des agents du FRA[37] ou, dans le cas du chancelier, en octroyant une réparation.

V. LA TRANSMISSION DES DONNÉES INTERCEPTÉES À DES SERVICES DE RENSEIGNEMENT ÉTRANGERS

20. Concernant la transmission des données interceptées à des tiers étrangers, la seule garantie offerte par la loi est l'exigence de l'intérêt national que doit présenter la transmission en question. Il n'existe aucune obligation de prendre en compte le possible impact de la mesure sur le droit au respect de la vie privée de la personne concernée ou d'obliger l'État destinataire à protéger les données par des garanties similaires à celles applicables en Suède. Lorsque la loi encadrant la compétence du service d'interception emploie des termes si vagues et que le contrôle se borne à vérifier que ledit service n'outrepasse pas son domaine de compétence, le contrôle exercé n'est pas très utile[38].

21. L'argument du Gouvernement selon lequel la coopération internationale est subordonnée au respect par l'État destinataire de la législation suédoise n'est étayé par aucune disposition législative interne. Le Gouvernement ne se réfère, en effet, qu'aux « directives générales du FRA »[39]. En vertu du droit applicable, le FRA est seulement tenu d'informer l'Inspection du renseignement extérieur des principes régissant sa coopération avec des tiers étrangers, de préciser les pays et les organisations internationales auxquels les données sont communiquées et de

---

[36] Paragraphe 64 du présent arrêt.

[37] Paragraphes 66-68 du présent arrêt.

[38] La législation suédoise est bien éloignée de la norme universelle décrite 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, adoptée par les Nations unies le 17 mai 2010 (A/HRC/14/46) : « Pratique n° 31 : Le partage de renseignements entre différents services de renseignement d'un même État ou avec les autorités d'un autre État est fondé sur une loi nationale qui définit les paramètres de l'échange de renseignements, et notamment les conditions devant être réunies pour que des informations puissent être partagées, les instances avec lesquelles le partage de renseignement est permis et les garanties entourant l'échange de renseignements. » Voir aussi les pratiques n^{os} 32-35.

[39] Paragraphe 216 du présent arrêt.

fournir des informations générales concernant les opérations. Étant donné qu'aucun autre organe n'est investi de pouvoirs permettant d'exercer un véritable contrôle afin de s'assurer que la coopération avec des services de renseignement étrangers n'est pas utilisée pour contourner le droit national et que les États destinataires protègent les données par des garanties identiques ou similaires à celles applicables en droit suédois, le contrôle exercé par l'Inspection sur les activités du FRA en matière de coopération internationale, invoqué par le Gouvernement, est sans incidence[40].

22. La position du Gouvernement est d'autant moins acceptable qu'elle est en contradiction avec les obligations internationales de la Suède, vis-à-vis non seulement de l'Union européenne[41] mais aussi du Conseil de l'Europe. Outre la Convention, 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), que la Suède a ratifié, prévoit que les parties doivent garantir un niveau de protection adéquat pour les transferts de données à caractère personnel vers un pays tiers et que des dérogations ne sont possibles que lorsque des intérêts légitimes prévalent. Le rapport explicatif dudit Protocole additionnel ajoute que les exceptions doivent être interprétées de manière restrictive « afin que l'exception ne devienne pas la règle » (§ 31). Or, en Suède, l'exception est la règle.

VI. CONCLUSION

23. En somme, les organes de contrôle suédois ne satisfont pas à l'exigence d'une indépendance suffisante, ou n'assurent pas un contrôle efficace, ou les deux à la fois. Avec sa procédure occulte et ses décisions secrètes et non susceptibles de recours, le tribunal pour le renseignement extérieur n'est pas une juridiction administrant la justice au nom du peuple suédois et responsable devant lui. Il s'agit d'une commission secrète composée de représentants politiques, qui produit un diktat confidentiel non

[40] Voir aussi les Observations finales concernant le septième rapport périodique de la Suède (précitées, § 36), dans lesquelles le Comité des droits de l'homme des Nations unies s'est dit préoccupé par « l'absence de garanties suffisantes contre les atteintes arbitraires au droit à la vie privée en ce qui concerne l'échange de données brutes avec d'autres agences de renseignement ».

[41] FRA de l'UE, Surveillance par les services de renseignement, précité, p. 11 : « Les États membres devraient définir des règles concernant les modalités d'échange international du renseignement. Les organes de contrôle devraient contrôler ces règles et déterminer si les procédures de transfert et de réception des informations de renseignement respectent les droits fondamentaux et incluent des garanties adéquates. (…) Les États membres devraient veiller à ce que leur législation relative à la coopération en matière de renseignement définisse clairement l'étendue des compétences des organes de contrôle dans le domaine de la coopération entre services de renseignement. »

susceptible de recours. Ce tribunal ne poursuit qu'un seul but : blanchir les choix du FRA, qui sont en réalité les choix du gouvernement en matière de politique de surveillance, en donnant aux Suédois l'impression trompeuse qu'il existe un tribunal à Stockholm qui veille au respect du droit à la vie privée.

24. L'Inspection du renseignement extérieur n'est pas mieux. Lorsqu'on lui demande de vérifier si l'interception et le traitement des communications ont été effectués dans le respect du droit applicable, elle décide *in causa sua*, sans même devoir informer le plaignant de ses conclusions ou motiver ses décisions. Le plaignant est traité comme un sujet privé de tout droit au respect de la vie privée aux mains d'un État kafkaïen tout-puissant, et non comme une personne titulaire de droits opposables à l'État.

25. Le partage indiscriminé de données avec des services de renseignement étrangers, auquel la Suède procède, est plus dangereux pour les droits civils et le régime démocratique qu'un système de partage ciblé.

26. Au lieu de multiplier les organes de contrôle disposant de pouvoirs virtuels, il serait plus sage d'instituer une juridiction totalement indépendante, composée de juges expérimentés qui disposeraient du pouvoir d'exercer un contrôle efficace de bout en bout sur le processus d'interception, c'est-à-dire autoriser et superviser régulièrement la mise en œuvre de mesures d'interception en masse ciblées et fondées sur un soupçon, et faire cesser la collecte et la conservation illicites des données interceptées, en ayant accès aux documents classifiés nécessaires à l'exercice de leurs fonctions[42].

27. Les arguments concernant la difficulté pratique de mettre en œuvre les critères énoncés ci-dessus doivent être purement et simplement rejetés. Il ne s'agit pas en l'espèce d'une question d'efficacité pratique mais de prééminence du droit. C'est la loi qui fixe les limites d'un service public efficace, et non l'inverse. Mais on ne peut s'en apercevoir que si l'on se place, comme le fait le Voyageur de Caspar David Friedrich, au-dessus de la mer de nuages qui enveloppe le discours du Gouvernement.

[42] Voir mon opinion séparée jointe à l'arrêt *Big Brother Watch et autres*, précité, où les conditions pour qu'un régime d'interception en masse soit considéré comme conforme à la Convention sont discutées.

DECLARATION DE VOTE COMMUNE AUX JUGES KJOLBRO ET WENNERSTRÖM

(Traduction)

1. Nous avons voté en faveur d'un constat de non-violation de l'article 8 de la Convention et, par conséquent, nous ne souscrivons ni à la motivation ni aux conclusions de la Cour concernant le partage de renseignements (§§ 317-330) et le contrôle a posteriori (§§ 354-364).

2. Compte tenu de la nature de la question tranchée par la Cour, de l'importance de l'arrêt rendu par celle-ci, de la large majorité en faveur d'un constat de violation de l'article 8 de la Convention et de la motivation de l'arrêt adopté à l'unanimité par la chambre, nous nous abstiendrons de développer nos arguments juridiques dans cette affaire et nous limiterons à la présente déclaration de vote.