Strasbourg, 15 décembre 2015 **CDL-AD(2015)011**

Etude n° 719/2013 Or. angl.

COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT

(COMMISSION DE VENISE)

RAPPORT

SUR LE CONTRÔLE DÉMOCRATIQUE DES AGENCES DE COLLECTE DE RENSEIGNEMENTS D'ORIGINE ÉLECTROMAGNÉTIQUE

Adopté par la Commission Venise
lors de sa 102e session plénière
(Venise, 20-21 mars 2015)

sur la base des observations de

M. Iain Cameron (membre, Suède)

TABLE DE MATIERES

Résumé général

1. *Portée de l'étude.* Les processus de mondialisation et l'invention d'internet ont brouillé la distinction entre les menaces internes et externes pour la sécurité. Certains acteurs non étatiques peuvent poser de graves menaces. Par conséquent, la supervision des services de renseignement a beaucoup évolué au cours des dernières années, notamment dans la mesure où le renseignement d'origine électromagnétique (souvent désigné par l'acronyme ROEM) ne vise plus uniquement des renseignements relatifs à des menaces militaires extérieures mais relève aussi jusqu'à un certain point de la sécurité intérieure. Par conséquent, le ROEM peut désormais englober la surveillance « de télécommunications ordinaires » et fait peser un risque potentiel beaucoup plus important sur les droits individuels. L'organisation de cette activité de renseignement peut revêtir différentes formes selon les pays. Le présent résumé aborde les questions pertinentes de manière générale et ne saurait être interprété comme suggérant que tous les États se conforment à un modèle particulier de ROEM ou réglementent cette activité d'une certaine manière.

2. *Est-il nécessaire d'améliorer le contrôle démocratique ?* La surveillance stratégique implique l'accès à la fois au contenu des liaisons internet et des télécommunications, et aux métadonnées (à savoir toutes les données ne faisant pas partie du contenu d'une communication). Elle commence par l'affectation au service de ROEM d'une mission consistant à réunir des renseignements sur un phénomène ou bien sur une personne ou un groupe de personnes. Les très grosses quantités de données de contenu et de métadonnées ainsi obtenues sont ensuite filtrées et collectées de diverses manières ; l'essentiel d'entre elles est soumis à une analyse informatique effectuée sur la base de « sélecteurs » qui permettent de choisir une langue, des personnes, des mots-clés relatifs au contenu (par exemple le nom de produits industriels), des schémas de communication et/ou d'autres données techniques.

3. À la différence de la surveillance « ciblée » (interception secrète de conversations par des moyens techniques (mise sur écoute) du contenu des télécommunications et de métadonnées), la surveillance stratégique n'est pas forcément déclenchée en raison d'un soupçon pesant sur une ou plusieurs personnes spécifiques. Le ROEM vise à permettre aux responsables de la politique extérieure et/ou des armées ou de la sécurité stratégique de prendre des décisions en connaissance de cause et non pas nécessairement d'enquêter sur des menaces pour la sécurité intérieure. Il comporte donc un élément proactif puisqu'il vise à trouver ou à identifier un danger au lieu de se contenter d'enquêter sur une menace connue. Cette caractéristique explique la valeur qu'il peut revêtir au regard des opérations de sécurité, mais aussi les risques qu'il peut comporter pour les droits individuels.

4. Les services de ROEM bénéficient généralement d'une part substantielle du budget alloué au renseignement, tandis que les systèmes censés les contrôler semblent généralement réduits à la portion congrue. Plusieurs raisons expliquent cette dissemblance. Premièrement, d'aucuns avancent que l'accès à de simples métadonnées ne saurait sérieusement porter atteinte à la vie privée, pas plus que l'accès aux données de contenu, dans la mesure où cette opération est effectuée par des logiciels de recherche (« sélecteurs »). Aujourd'hui, pourtant, les métadonnées peuvent révéler beaucoup de détails sur la vie privée d'une personne et les sélecteurs de contenu être conçus de manière à collecter des informations sur certains individus ou groupes spécifiques. Deuxièmement, alors que jadis l'essentiel des télécommunications transitait par les ondes radio, à savoir une technologie généralement moins susceptible de faire naître de grandes attentes en matière de respect de la vie privée, il emprunte désormais des câbles en fibre optique. Troisièmement, la surveillance stratégique visant les communications extérieures, d'aucuns avancent que seule la vie privée de personnes n'étant ni des ressortissants ni des résidents est affectée ; toutefois, à supposer même qu'on laisse de côté la question de la légitimité d'une telle distinction au regard de la Convention européenne des droits de l'homme

(CEDH), il est impossible pour des raisons techniques d'éviter le mélange des communications intérieures et extérieures et, par conséquent, le risque de contourner les contrôles domestiques plus stricts pouvant peser sur la surveillance « ordinaire ». Quatrièmement, les contrôles tendent à faiblir en raison de la complexité technique et de la rapidité des progrès technologiques dans ce domaine. Il convient pourtant d'avoir à l'esprit que, si l'absence de réglementation de ce secteur devait persister, c'est au service de renseignement lui-même – et non à la législature – qu'il appartiendrait de veiller au maintien de l'équilibre nécessaire entre les impératifs inhérents à sa mission et la protection des droits individuels, au risque de favoriser la collecte. Cinquièmement, divers facteurs – tels que la croissance trop rapide des services de ROEM, les progrès fulgurants de la technologie, la perte de la mémoire institutionnelle ou des pressions politiques en vue d'obtenir des résultats rapides – pourraient exercer une influence néfaste sur l'intégrité et le professionnalisme du personnel. Enfin, le ROEM relève d'un réseau coopératif international et, par conséquent, génère des problèmes spécifiques en matière de contrôle.

5. La surveillance stratégique n'est pas forcément une surveillance « massive », mais peut le devenir lorsque la collecte porte sur des données en vrac et que les seuils d'accès correspondants sont bas. Les services de ROEM disposent généralement de ressources informatiques très puissantes et sont donc en mesure de porter atteinte à la vie privée et à d'autres droits individuels. Ils devraient par conséquent faire l'objet d'une réglementation adéquate en vertu du principe de l'État de droit.

6. *Juridiction.* Même si la collecte de ROEM peut légitimement avoir lieu sur le territoire d'un État tiers avec son consentement, elle peut malgré tout engager la responsabilité de l'État collecteur sous l'angle du respect par celui-ci des obligations que lui confère la CEDH en matière de protection des droits de l'homme. De toute façon, le traitement, l'analyse et la communication de ce matériel relèvent clairement de la juridiction de l'État collecteur et sont régis à la fois par la législation interne et les normes applicables en matière de protection des droits de l'homme. Les obligations imposées par ledit État aux entreprises de télécommunication sont parfois en concurrence, voire en contradiction, avec les obligations qui pèsent sur les mêmes entreprises en matière de protection des données en vertu du droit du pays où s'exerce la surveillance ; la définition de normes internationales minimales apparaît donc d'autant plus indispensable.

7. *Contrôle – Contexte organisationnel.* Le ROEM est une activité onéreuse et requiert des compétences techniques extrêmement pointues. Par conséquent, même si tous les États développés sont contraints aujourd'hui d'assumer une fonction défensive en matière de cyber-sécurité, seuls quelques-uns disposent d'une capacité de collecte offensive sous la forme d'un service spécialisé ou d'une mission confiée en la matière à l'organisme chargé du renseignement extérieur.

8. *Forme du mandat.* La plupart des États démocratiques ont défini au moins partiellement les modalités du ROEM dans leur législation primaire, conformément aux exigences posées par la CEDH. Des normes ou des lignes directrices plus détaillées sont normalement énoncées dans la législation secondaire, que celle-ci soit sous forme de décrets d'application pris par l'exécutif (et rendus publics) ou de circulaires émanant du directeur du service compétent (et gardées secrètes). Cette façon de procéder risque de générer des problèmes sous l'angle de la qualité de la loi (prévisibilité, etc.).

9. *Contenu du mandat.* Le mandat d'un service de ROEM peut être défini en termes très vagues de manière à permettre la collecte de données « pertinentes », « relatives à des services de renseignement étrangers » ou « présentant un intérêt » au regard d'enquêtes antiterroristes. Un mandat aussi large accroît le risque de collecte excessive. À supposer que la documentation justificative soit en outre inadéquate, le contrôle devient très difficile.

10. La collecte de renseignements pour « le bien-être économique de la nation » peut aboutir à un espionnage industriel. La surveillance stratégique est cependant utile dans au moins trois domaines d'activité économique : la prolifération des armes de destruction massive (et, en règle générale, la violation des interdictions d'exportation), le contournement des sanctions imposées par l'ONU et l'UE et le blanchiment de capitaux à grande échelle. L'interdiction claire de pratiquer l'espionnage économique – renforcée par un contrôle strict et la prohibition, pour les services de renseignement, d'accepter de se voir confier des missions par l'exécutif ou les services administratifs chargés de promouvoir le commerce – constituerait un mécanisme de prévention utile de ce point de vue.

11. Les États procèdent souvent entre eux à des transferts de données en vrac. Il serait utile, en vue d'éviter le contournement des règles relatives à la collecte dans le cadre du renseignement intérieur, de prévoir que les informations ainsi transférées ne puissent faire l'objet d'une analyse que si les conditions matérielles pesant sur toute investigation au niveau national sont réunies et si les mêmes autorisations que celles requises pour ces dernières ont été obtenues.

12. *Contrôle et attribution de tâches par le gouvernement.* L'identité des personnes ou organes chargés d'attribuer les tâches de surveillance dépendent de la nature des renseignements recherchés (diplomatique, économique, militaire et domestique) et les intéressés ne devraient pas être perçus comme des contrôles externes.

13. *Contrôle du réseau.* En raison de leur situation géographique et de la nature d'internet, les États collectent fréquemment des données présentant un intérêt pour d'autres ou bien ont accès à différentes parties d'un même message. Les liens entre pays alliés en matière de ROEM peuvent être extrêmement étroits. La règle dite « de la maîtrise de l'information par son auteur » risque donc de gêner considérablement le contrôle et ne devrait pas s'appliquer aux organismes compétents.

14. *Contrôle et jurisprudence de la Cour européenne des droits de l'homme.* La CEDH se compose de normes minimales et doit être perçue uniquement comme un point de départ pour les États européens censés offrir des garanties plus étendues. La Cour européenne des droits de l'homme (la Cour) n'a pas formulé la définition de la notion de sécurité nationale, mais a toutefois progressivement clarifié sa portée légitime. Dans sa jurisprudence relative aux mesures secrètes de surveillance, elle a énoncé des garanties minimales qui doivent être reprises dans le droit interne de manière à éviter les abus de pouvoir : la nature des infractions pouvant justifier une ordonnance d'interception ; la définition des catégories de personnes susceptibles de voir leur téléphone placé sur écoute et la durée maximale de cette mise sur écoute ; la procédure à suivre pour examiner, utiliser et conserver les données obtenues ; les précautions à prendre en cas de communication des données à d'autres parties ; et les circonstances dans lesquelles un enregistrement peut ou doit être effacé ou bien une bande détruite.

15. La jurisprudence de la Cour en matière de surveillance stratégique est pour l'instant très succincte, même si une partie des jurisprudences nationales et de la pratique des organismes de contrôle se fonde sur la CEDH. Plusieurs normes liées à la surveillance ordinaire ont dû être adaptées afin de pouvoir s'appliquer également à la surveillance stratégique. La première garantie (applicable uniquement aux États autorisant le recours au ROEM pour enquêter sur des infractions pénales) tient à l'énumération exhaustive des infractions pouvant donner lieu à une enquête reposant sur la collecte de renseignements d'origine électromagnétique, de sorte qu'il convient de prévoir la destruction des données relatives à d'autres infractions ayant pu être incidemment collectées. L'exception de transfert de données aux autorités répressives devrait être étroitement circonscrite et soumise à un contrôle.

16. Une autre garantie repose sur la définition des catégories de personnes dont les communications peuvent faire l'objet d'une interception. Le pouvoir de construire un graphe social (c'est-à-dire d'identification des personnes en contact l'une avec l'autre) devrait être plus étroitement circonscrit que par la simple « pertinence » ; le recours aux métadonnées à cette fin ne devrait normalement être possible que si le processus vise des personnes soupçonnées de participer réellement à des infractions pénales particulièrement graves comme le terrorisme. À supposer que le législateur considère néanmoins indispensable de conférer de larges pouvoirs en matière de construction de graphes sociaux, l'utilisation desdits pouvoirs devrait faire l'objet d'un contrôle strict, y compris au niveau de la procédure.

17. Les recherches portant sur les données de contenu peuvent avoir des implications importantes sur la vie privée, dès lors qu'on envisage d'utiliser un sélecteur associé à une personne physique (par exemple son nom, son surnom, son adresse électronique, son adresse physique, etc.). Il convient de renforcer l'exigence d'une justification et les garanties procédurales telles que la participation d'un défenseur de la vie privée. Des garanties devraient également être mises en place en ce qui concerne les décisions subséquentes de transfert des renseignements obtenus sur la base d'une surveillance stratégique à des organismes chargés de la sécurité intérieure, à des autorités répressives ou à des services étrangers.

18. L'interception de communications privilégiées au moyen de la collecte de ROEM est particulièrement problématique, de même que l'exploitation des renseignements ainsi obtenus contre des journalistes, de manière à identifier leurs sources. Des méthodes devraient être élaborées afin de conférer aux avocats, journalistes et autres communicants privilégiés une certaine protection, sous la forme par exemple d'un seuil élevé ou très élevé en matière d'approbation d'opérations de collecte contre les intéressés, seuil auquel viendraient s'ajouter des garanties procédurales et un contrôle externe strict.

19. La garantie consistant à fixer un délai n'est pas aussi solide en matière de surveillance stratégique qu'en matière de surveillance ordinaire. Les périodes de surveillance tendent en effet à s'allonger et le délai à être systématiquement reconduit. Le délai de conservation a tendance, lui aussi, à s'allonger : des données initialement considérées comme sans intérêt peuvent, à la lumière de nouvelles données, apparaître pertinentes. Il pourrait s'avérer opportun d'exiger de procéder périodiquement à une vérification interne de la nécessité (persistante) de conserver les données. Cette vérification, pour être efficace, devrait pouvoir s'appuyer sur un contrôle externe.

20. Le ROEM comporte deux étapes importantes pendant lesquelles des garanties doivent s'appliquer : le processus d'autorisation et le processus de suivi (contrôle). Le second doit obligatoirement relever d'un organisme indépendant et extérieur comme cela résulte clairement de la jurisprudence de la Cour européenne des droits de l'homme. La question qui se pose en l'occurrence est de savoir si le processus d'autorisation devrait lui aussi être indépendant.

21. *Contrôle interne et contrôle gouvernemental, éléments de systèmes de contrôle globaux.* Même s'il est particulièrement tentant de se reposer principalement sur les contrôles internes en matière de surveillance stratégique, lesdits contrôles sont insuffisants. Il convient de renforcer considérablement le contrôle externe du ROEM.

22. *Contrôle par le parlement.* Plusieurs raisons expliquent le caractère problématique du contrôle parlementaire de la surveillance stratégique. Les parlementaires ont souvent du mal à trouver le temps nécessaire pour exercer ce contrôle, d'autant que la surveillance stratégique suppose une expertise technique qu'ils n'ont pas et qui est indispensable pour comprendre ce domaine. La collaboration en réseau entre les services de ROEM rend également difficile un contrôle parlementaire susceptible d'affecter les services de pays

étrangers. Toutes ces difficultés peuvent être surmontées, mais, plus problématique encore, la surveillance stratégique implique une ingérence dans les droits individuels. Le contrôle de telles mesures relevait généralement du pouvoir judiciaire.

23. La prise de décision d'utiliser des sélecteurs particuliers s'apparente, du moins sur certains points, à une décision d'autorisation d'une surveillance ciblée. À ce titre, elle peut être prise par un organe juridictionnel hybride qui réunit les compétences des services judiciaires et de politique étrangère. En ce qui concerne le suivi (contrôle), il est nécessaire de superviser les décisions rendues par des systèmes automatisés de manière à effacer les données non pertinentes, ainsi que les décisions prises par des analystes en chair et en os en vue de conserver les renseignements à caractère personnel collectés et de les transférer à d'autres services nationaux ou étrangers. Ce type de contrôle s'apparente à une « protection des données » et peut être utilement confié à un organe administratif indépendant et spécialisé, qui pourra, et devra, rendre des comptes au parlement.

24. *Autorisation juridictionnelle.* Tout système d'autorisation doit être complété par une forme de contrôle de suivi visant à vérifier le respect des conditions. Cette mesure s'impose à la fois parce que le processus d'affinage des sélecteurs est dynamique et très technique, et également parce que les juges voient peu le résultat des opérations de ROEM, puisque celles-ci débouchent rarement sur des poursuites. Par conséquent, les garanties applicables à un procès pénal ne sont jamais mises en œuvre.

25. *Contrôle par des organes spécialisés*. La distinction entre les organes parlementaires, juridictionnels et spécialisés est loin d'être évidente ; dans certains États, les organes de contrôle comportent ces trois éléments à la fois. Les organes spécialisés ont un rôle particulier à jouer dans la mesure où ils doivent vérifier que les activités de ROEM sont menées conformément à des normes élevées de protection des données.

26. *Mécanisme de traitement des plaintes.* En vertu de la CEDH, tout État doit offrir à ses justiciables un recours effectif en cas de violation alléguée de leurs droits. L'article 8 de cet instrument n'impose pas expressément de notifier aux intéressés qu'ils ont fait l'objet d'une surveillance stratégique. Lorsque le droit interne prévoit une procédure générale de recours devant un organe de contrôle indépendant, ce mécanisme peut compenser l'absence de notification. Un recours ne peut être qualifié d'effectif que si certaines conditions sont respectées.

27. *Remarques conclusives.* Les États ne devraient pas se contenter des normes minimales énoncées par la CEDH. Le ROEM présente un risque potentiel élevé d'ingérence dans le droit à la vie privée et l'exercice d'autres droits individuels. Il peut être réglementé de manière souple (à savoir que de nombreuses personnes sont attrapées dans les mailles du filet et que les renseignements les concernant sont conservés) ou relativement rigide (à savoir que la violation réelle du droit à la vie privée et des autres droits individuels est réduite au minimum). Les modèles suédois et allemand présentent des avantages indéniables par rapport aux autres modèles étudiés dans ce contexte. En tout cas, il est nécessaire de définir légalement les principaux éléments de la collecte et de prévoir de solides mécanismes de contrôle. Le législateur national doit se voir conférer une réelle possibilité de comprendre la matière et d'assurer les équilibres nécessaires.

I. Introduction

28. En 2007, à l'invitation du Comité des Ministres du Conseil de l'Europe, la Commission de Venise a adopté un « Rapport sur le contrôle démocratique des services de sécurité » (CDL-AD(2007)016, ci-après le « Rapport 2007 »).

29. En novembre 2012, la commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe a demandé à la Commission de Venise de préparer une mise à jour dudit rapport. M. Iain Cameron (membre, Suède) a été désigné comme rapporteur.

30. En mai 2013, une demande a été adressée à tous les membres de la Commission de Venise concernant l'évolution des questions pertinentes en matière de contrôle de la sécurité intérieure. Des informations ont été alors communiquées par M. Sörensen (membre, Danemark), M. Haenel (membre, France) et M. Hoffmann-Riem (membre, Allemagne). Des informations utiles ont également été communiquées par M[me] Sarah Cleveland (membre, États-Unis) et le professeur Martin Scheinin (ancien rapporteur spécial des Nations Unies sur le terrorisme et les droits de l'homme et représentant de l'AIDC [Association internationale de droit constitutionnel] à la Commission de Venise) entre mars 2011 et juin 2014[1].

31. Au cours de l'automne 2014, M. Cameron et le réseau d'experts de l'Agence des droits fondamentaux ont procédé à un échange de vues sur les services nationaux de renseignement et leur contrôle dans l'Union européenne dans le cadre d'un projet intitulé « Droits fondamentaux, garanties et recours ».

32. Le présent rapport a été discuté lors de la réunion de la sous-commission des institutions démocratiques tenue le 19 mars 2015 et adopté par la suite par la Commission de Venise lors de sa 102[e] session plénière (Venise, 20-21 mars 2015).

II. Portée de la présente étude : définitions

33. L'évolution la plus importante, depuis l'adoption d'étude de la Commission réalisée en 2007 sur le contrôle démocratique des services de sécurité tient au renseignement d'origine électromagnétique. Le ROEM est un terme générique désignant les moyens et méthodes permettant d'intercepter et d'analyser des communications transmises par ondes radio (y compris sur des réseaux satellite et de téléphonie mobile) et par câbles. Traditionnellement, le ROEM servait principalement à obtenir des renseignements militaires (intéressant la défense) et, accessoirement, à obtenir des renseignements intéressant les relations extérieures ou l'activité diplomatique. Il relevait donc principalement des services de renseignement militaire extérieur. Toutefois, en raison des processus de mondialisation et de l'apparition d'internet, la distinction entre sécurité intérieure et extérieure tend à s'estomper. En outre, au moins depuis les attaques terroristes du 11 septembre 2001, il est devenu évident que même des acteurs non étatiques peuvent faire peser de lourdes menaces sur la sécurité nationale[2]. Comme cela est expliqué plus en détail dans la

[1] Le rapporteur tient également à témoigner sa gratitude à M. Douglas Cantwell pour ses commentaires et informations utiles relatifs au droit et à la pratique des États-Unis, ainsi qu'à M[me] Hilde Bos pour ses informations sur les pratiques néerlandaises en matière de contrôle.

[2] Voir le paragraphe 64 du rapport de 2007 ; voir aussi le document intitulé « , , Liberty and Security in a Changing World, Report and Recommendations by the President's Review Group on Intelligence and Communications Technologies », 12 décembre 2013, p. 177. Ce rapport remet également en question, de manière plus controversée, la pertinence du maintien de la distinction entre les situations de conflit armé et de paix.

section qui suit, le ROEM exerce désormais un impact considérable sur la sécurité intérieure, ainsi que sur l'exercice de droits individuels.

34. Les termes « surveillance stratégique » servent fréquemment à indiquer que le ROEM peut aujourd'hui inclure la surveillance des « communications ordinaires » et c'est avec cette acception qu'ils sont utilisés dans le présent rapport[3]. Les éléments militaires du ROEM (c'est-à-dire le suivi de la répartition des forces armées étrangères, de leur état de préparation, etc.), même s'ils représentent peut-être encore une part essentielle des fonctions du service compétent[4], ne sont pas analysés dans le présent rapport[5].

35. Les termes « service de ROEM » sont parfois utilisés dans le présent rapport. Comme indiqué *infra* dans la section V.C, la tâche de collecte et de surveillance stratégiques a beau pouvoir être confiée à divers types d'organes, nous nous sommes attachés à traiter de la fonction, quelle que soit la manière dont elle est organisée. Si tous les États disposent d'une fonction de sécurité intérieure, certains d'entre eux ne disposent pas des ressources requises pour assumer la fonction de surveillance stratégique ou bien n'en éprouvent pas le besoin. Les observations relatives aux meilleures pratiques dans ce domaine s'adressent donc principalement aux États gérant cette fonction.

36. Le rapport sur le contrôle démocratique des agences de renseignement d'origine électromagnétique devrait être lu conjointement avec le rapport de 2007, mis à jour en 2015 (CDL-AD (2015) 010), qui expose en détail les principes généraux de la surveillance de la sécurité.

III. Un contrôle démocratique (amélioré) est-il nécessaire ?

A. Qu'est-ce que la surveillance stratégique ?

37. Le rapport de 2007 met l'accent sur le contrôle des services de sécurité. Il commence par expliquer brièvement l'objet du contrôle et les raisons de celui-ci. En d'autres termes, il explique comment ces services collectent et analysent des renseignements. Les services de sécurité intérieure ont notamment recours à l'interception clandestine des conversations par des moyens techniques (écoutes téléphoniques), ainsi qu'à la collecte secrète du contenu des télécommunications et de métadonnées[6]. Il conviendrait d'élargir cet exercice de définition à la surveillance stratégique.

---

[3] Conformément à la législation allemande pertinente, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) à savoir la loi restreignant le caractère privé de la correspondance, des postes et des télécommunications, telle qu'elle a été adoptée le 26 juin 2001 (*Journal officiel fédéral I*, p. 1254, revision 2298) modifiée pour la dernière fois par l'article 1 de la loi du 31 juillet 2009 (*Journal officiel fédéral I*, p. 2499 (ci-après « la loi G10 »). Cette terminologie a également été adoptée par la Cour européenne des droits de l'homme (voir, *infra*, la section VI). Toutefois, dans le présent rapport, ce terme se voit attribuer une acception légèrement plus large que dans la législation allemande, de manière à couvrir également le recours aux renseignements d'origine électromagnétique en vue de collecter des informations sur des individus ou des groupes identifiés.

[4] Par exemple, le service de ROEM (renseignement d'origine électromagnétique) suédois, Försvarets Radio Anstalt (FRA), estime qu'au moins 50 % de son travail revêt un caractère militaire.

[5] Ce qui semble approprié dans la mesure où l'article 1.*d* du Statut du Conseil de l'Europe prévoit que les questions relatives à la défense nationale ne sont pas de la compétence de l'Organisation. Les utilisations militaires du ROEM peuvent générer des problèmes sous l'angle des droits de l'homme, notamment lorsque les données produites par la surveillance stratégique constituent la base d'une réplique militaire à une agression commise par une entité non étatique, notamment sous la forme d'une attaque par drone de personnes soupçonnées de terrorisme. Cette question n'est cependant pas examinée dans le cadre du présent rapport.

[6] Pour simplifier, les métadonnées sont « des données relatives aux données ». Dans le contexte des télécommunications, ce terme désigne généralement toutes les données ne faisant pas partie du contenu de la communication (même si la distinction entre données de contenu et métadonnées n'est pas toujours claire). À

38. Toutes ces méthodes de surveillance, telles qu'elles sont utilisées par les services de sécurité intérieure, sont « ciblées » au sens où elles partent de l'hypothèse qu'une ou plusieurs personnes ont commis, commettent ou projettent de commettre une infraction contre la sûreté de l'État, ou bien – concernant les pays ne limitant pas le mandat de leurs services de sécurité aux enquêtes pour infraction – observent une conduite s'analysant en une menace pour la sécurité nationale. L'ensemble de ces méthodes entre en conflit avec l'article 8 de la CEDH et d'autres droits individuels, de sorte que la loi prévoit le seuil au-delà duquel il est permis de déclencher une surveillance : il faut des faits concrets attestant d'une conduite s'analysant en une infraction pénale ou en une menace pour la sécurité et les enquêteurs doivent « avoir un motif probable de suspicion », « nourrir un soupçon raisonnable » ou remplir un autre critère analogue.

39. La décision d'autoriser la surveillance est généralement prise par une personne ou un organe exclu de la gestion au jour le jour de l'enquête ; il s'agit le plus souvent d'un tribunal, mais, dans certains pays, cette fonction est assumée par un procureur, voire un ministre du gouvernement. La permission est limitée à la surveillance d'une ou plusieurs personnes, ou bien d'un endroit spécifique, et n'est accordée que pour une durée précise. La procédure devant l'organe ou la personne chargé d'octroyer l'autorisation est toujours secrète. En ce qui concerne les interceptions du contenu des communications ou des métadonnées dans le cadre d'une opération visant la sécurité intérieure ou l'activité des autorités répressives, l'entreprise de télécommunication concernée reçoit l'ordre de faciliter l'interception ou de remettre les métadonnées. À supposer que la surveillance des télécommunications, ainsi que d'autres éléments, permette de réunir suffisamment de preuves de la participation à un crime contre la sécurité, des poursuites peuvent être engagées. Le matériel intercepté sera alors considéré (dans la plupart des États) comme une preuve recevable. Lorsque les preuves qu'une infraction a été ou est commise pèchent par leur insuffisance, mais que des soupçons raisonnables subsistent, l'enquête peut continuer. Les enquêtes relevant de la sécurité tendent à durer plus longtemps que les enquêtes ordinaires menées par les autorités répressives. Lorsqu'une enquête impliquant une surveillance prend fin, il est obligatoire dans bon nombre d'États de le notifier – passé un certain délai – à la personne surveillée (à moins qu'une telle mesure ne fasse peser un risque de divulgation des méthodes d'enquête ou des sources).

40. Des garanties ont été mises en place à différentes étapes de la procédure de manière à toujours assurer un équilibre entre le respect des droits de l'homme et l'efficacité de l'enquête visant un crime ou une menace contre la sécurité nationale, de manière à réduire autant que faire se peut l'ingérence dans ces droits et à limiter la portée des abus de pouvoir éventuels.

41. Les garanties mises en place autour de l'obtention de métadonnées dans le cadre d'une enquête criminelle ou de la sécurité intérieure tendent à être moins complètes que celles applicables aux écoutes ou à l'interception du contenu des télécommunications, dans la mesure où l'accès à ces données présenterait moins de risques d'ingérence dans la vie privée et les autres droits individuels.

42. La surveillance stratégique implique à la fois l'accès au contenu des liaisons internet et des télécommunications et aux métadonnées. Elle commence par l'affectation au service de ROEM d'une mission consistant à réunir des renseignements sur un phénomène ou bien sur une personne ou un groupe de personnes donné. Les très grosses quantités de données de contenu et de métadonnées ainsi obtenues sont ensuite filtrées et collectées de diverses

---

titre d'exemple, le numéro appelé, la durée de l'appel ou la localisation de l'appelant et de l'appelé sont des métadonnées.

manières[7]. L'essentiel d'entre elles est soumis à une analyse informatique effectuée sur la base de « sélecteurs »[8] qui permettent de choisir une langue, des personnes, des mots-clés relatifs au contenu (par exemple le nom de produits industriels), des schémas de communication et/ou d'autres données techniques. Cette étape est l'une des plus importantes sous l'angle de la mise en balance de la protection de la vie privée, d'une part, et des autres intérêts en présence, d'autre part. En pratique, la question de savoir si ce processus limite convenablement les intrusions superflues dans les communications personnelles innocentes revient à déterminer si le sélecteur est suffisamment pertinent et spécifique, et si la qualité de l'algorithme du logiciel employé pour identifier les données pertinentes dans le cadre des paramètres choisis est satisfaisante (voir cependant aussi, *infra*, le paragraphe 58).

43. Les métadonnées en vrac sont analysées de manière à identifier des schémas de communication. Ce processus revêt généralement la forme d'une vérification des appels passés ou reçus entre des numéros de téléphone suspects préalablement identifiés (X) et d'autres numéros (Y), puis entre ces derniers et un troisième groupe de numéros (Z) (dans le cadre de ce qu'il est convenu d'appeler « l'analyse des contacts en chaîne », en vue de construire un graphe social). Même si les enquêtes aux fins de sécurité intérieure ou de poursuite d'une infraction pénale ont toutes recours à des graphes sociaux construits sur la base d'une analyse de métadonnées, il peut exister des différences concernant à la fois la portée du graphe, la quantité des données traitées et les garanties applicables en matière de protection de la vie privée (voir la section VI).

44. Une fois la première recherche automatique par ordinateur terminée et après suppression des données superflues et affinage des autres, un analyste en chair et en os complète le dépouillement des renseignements en supprimant notamment le matériel considéré comme non pertinent (dans le cadre de ce qu'il est souvent convenu d'appeler « la minimisation »). Cette étape revêt, elle aussi, une grande importance sous l'angle de la mise en balance de la protection de la vie privée, d'une part, et des autres intérêts en présence, d'autre part. Le matériel résiduel fait ensuite l'objet d'une analyse supplémentaire avant d'être ajouté à d'autres renseignements pour générer un produit final qui sera ensuite conservé en vue d'une utilisation future, puis diffusé, etc.

45. L'organe pouvant demander au ROEM de produire les renseignements demandés est généralement déterminé par la législation primaire ou secondaire : il peut s'agir d'un ministre du gouvernement, d'un service de l'exécutif, des forces armées (ou d'une partie d'entre elles) ou bien d'un service de sécurité extérieure ou intérieure. La détermination des sélecteurs les plus susceptibles de produire les renseignements demandés revêt surtout un caractère technique et, à ce titre, le plus souvent laissée à la discrétion du service. Toutefois, compte tenu de l'impact que la collecte de renseignements en vrac et le recours aux sélecteurs peuvent avoir sur les droits individuels, plusieurs États disposent aujourd'hui d'un organe distinct chargé de délivrer les autorisations. Cet organe peut autoriser la

[7] Pour plus de détails techniques, voir M. Cayford, C. van Gulijk et P. H. A. J. M. van Gelder, « All swept up : An initial classification of NSA surveillance technology », *in* Nowakowski, T. *et al.* (éd.), *Safety and Reliability: Methodology and Applications*, Taylor and Francis, Londres, 2015, paru dans le cadre du projet de recherche Surveille. On peut trouver une explication du processus de renseignement d'origine électromagnétique dans son ensemble au chapitre 2 du rapport publié par le National Research Council of the National Academies, « Bulk Collection of Signals Intelligence : Technical Options », National Academy Press, 2015 (ci-après « le rapport du Conseil national de la recherche des États-Unis »).

[8] Le rapport du Conseil national de la recherche des États-Unis utilise le terme « discriminant » pour désigner les termes servant à filtrer la collecte ; le processus de collecte se déroulant en temps réel, les termes doivent être forcément plus simples que ceux (« les sélecteurs ») servant à effectuer des recherches dans les données collectées en vrac. Une « interrogation » des données collectées peut combiner plusieurs « sélecteurs » (*ibid.*, p. 38 et 39). Pour plus de simplicité, nous avons utilisé dans le présent rapport le terme « sélecteur » pour désigner les deux cas de figure.

collecte en vrac et/ou approuver la liste des sélecteurs qui seront utilisés dans le cadre d'une opération spécifique de collecte de renseignements. Il peut s'agir d'un ministre du gouvernement (souvent le même que celui ayant déjà affecté une mission au service) ou bien d'un organe extérieur présentant un caractère judiciaire ou quasi judiciaire.

46. Le processus de définition et d'affinage des sélecteurs est dynamique. Le service de ROEM teste constamment de nouvelles méthodes de recherche, des canaux de communication, etc., afin d'anticiper et de neutraliser les contre-mesures réelles ou potentielles adoptées par la cible. Il n'est pas rare que des renseignements utiles soient également obtenus dans le cadre de ces tests.

47. Par conséquent, la surveillance stratégique diffère sous plusieurs aspects de la surveillance exercée par les autorités répressives ou des opérations plus traditionnelles relevant de la sécurité intérieure. Elle n'est pas forcément déclenchée sur la base d'un soupçon à l'encontre d'une ou plusieurs personnes particulières et peut revêtir un caractère proactif : trouver un danger jusque-là inconnu plutôt qu'enquêter sur un danger connu. Cette caractéristique explique les avantages potentiels d'une telle surveillance au regard de la sécurité, mais également les risques qu'elle peut faire peser sur les droits individuels. Bien que la collecte des renseignements ne vise pas principalement à engager des poursuites, les informations récoltées sont conservées et se prêtent à diverses utilisations susceptibles d'affecter l'exercice de ces droits. Néanmoins, en dépit des différences entre la surveillance ciblée et la surveillance stratégique, il apparaît manifestement qu'il est possible de mettre en place ou de créer des garde-fous, à divers stades de la procédure, de manière à mettre en balance la protection de la vie privée et des autres droits individuels, d'une part, et l'efficacité des enquêtes visant les crimes ou menaces intéressant la sécurité nationale (de manière à réduire l'ingérence dans l'exercice desdits droits et à limiter les possibilités d'abus de pouvoir), d'autre part.

B. Le contrôle de la surveillance stratégique s'est-il relâché ?

48. Dans les États qui disposent d'un tel service, le ROEM tend à bénéficier d'une part substantielle du budget alloué à l'activité de renseignement, mais l'honnêteté commande de dire que le système de contrôle tend quant à lui à s'éroder. Plusieurs raisons peuvent être avancées pour expliquer cette évolution. La première a déjà été mentionnée et repose sur l'hypothèse selon laquelle la simple collecte de métadonnées n'affecte pas sensiblement la vie privée ; or, comme expliqué plus loin dans la présente section, ce raisonnement ne tient plus. En ce qui concerne l'impact sur la vie privée de l'accès aux données de contenu par le biais de l'interception des communications, d'aucuns ont fait valoir que, à la différence de l'écoute par un analyste en chair et en os d'une conversation téléphonique, l'analyse automatique par un logiciel de recherche (configuré d'une certaine manière à l'aide de sélecteurs) à des données en vrac ne constitue pas une ingérence dans la vie privée. Pourtant, cet argument est incorrect, au moins du point de vue des droits individuels : les sélecteurs sont en effet conçus par des personnes en chair et en os. Même si ceux qui visent à identifier un produit, tel qu'un précurseur chimique, n'ont pas d'impact direct sur les droits individuels, il en va autrement de ceux qui visent un individu ou un groupe[9].

[9] D'aucuns prétendent que l'ingérence dans la vie privée se produit non pas au moment de la collecte des données mais après le traitement automatisé de minimisation qui leur est appliqué. En effet, seules les données retenues à l'issue dudit traitement sont accessibles. Toutefois, la simple collecte des données peut affecter d'autres droits individuels (voir, *infra*, les paragraphes 62,63 et 92).

49. Une deuxième explication revêt un caractère historique et consiste à expliquer que les télécommunications internationales ont longtemps reposé sur la radio, à savoir une technologie généralement moins susceptible de faire naître de grandes attentes en matière de respect de la vie privée[10]. Aujourd'hui, cependant, la grande majorité des télécommunications nationales et internationales emprunte des câbles à fibres optiques et l'ampleur de ce trafic a énormément augmenté.

50. Une troisième explication fait ressortir le caractère initialement militaire du ROEM et, par conséquent, la priorité accordée par cette activité aux communications extérieures (étrangères). On pouvait donc jadis avancer que l'interception de communications extérieures affectait principalement la vie privée des non-ressortissants ou des non-résidents. La section V.C qui suit examine la question de la légitimité d'une telle distinction. Il convient de relever que la surveillance par un État des communications entre ses propres ressortissants et des étrangers implique forcément la surveillance des premiers. De toute façon, la plupart des télécommunications numériques sont désormais acheminées automatiquement selon la route la plus pratique et la moins onéreuse ou bien empruntent l'internet, de sorte que des communications considérées auparavant comme intérieures (c'est-à-dire établies entre des personnes vivant dans le même État) franchissent aujourd'hui fréquemment les frontières nationales. De même, toute communication avec un serveur étranger ou passant par un fournisseur de services internet (FAI) étranger peut être considérée dans un sens comme « internationale ». À supposer même qu'il soit possible de distinguer menaces intérieures et extérieures (ce qui, comme nous l'avons vu, devient de plus en plus ardu), la nature des télécommunications explique désormais qu'une quantité importante de communications « intérieures » risque d'être collectée dans le cadre des opérations visant à recueillir des communications « extérieures ». Ce mélange inévitable (pour des raisons techniques) de communications intérieures et extérieures constitue ainsi un argument de taille en faveur d'une amélioration du contrôle de la surveillance stratégique. En d'autres termes, nous sommes en présence d'un risque de contournement des contrôles nationaux plus stricts et des règles de suivi applicables à la surveillance « ordinaire » (voir, *infra*, la section V.C).

51. Une quatrième explication du relâchement des contrôles tient à la complexité des technologies utilisées et aux progrès fulgurants enregistrés dans ce domaine. Il est difficile pour un homme politique ou un juriste de comprendre la manière dont la surveillance stratégique s'exerce, peut affecter la vie privée ou d'autres droits individuels et permet la mise en place de freins et contrepoids. Lorsqu'un tel domaine d'activité demeure non réglementé, ce sont finalement les services de sécurité et de renseignement – et non le législateur – qui finissent par mettre en balance les différents intérêts en présence. En outre, comme indiqué dans le rapport de 2007, ces services ont naturellement tendance à vouloir obtenir davantage d'informations[11].

52. Cinquièmement, les prérogatives dont jouit l'exécutif dans de nombreux États en matière de définition des politiques étrangère et de défense – soit en vertu de la Constitution, soit *de facto* parce qu'il contrôle l'information pertinente – ont peut-être également contribué à l'absence de législation dans certaines juridictions. Cette raison renvoie à la troisième, à savoir qu'il est probable qu'un service conçu pour fournir des renseignements en vue de permettre l'élaboration en toute connaissance de cause d'une politique étrangère en général (et/ou l'adoption de décisions militaires/stratégiques) est perçu comme requérant une forme de surveillance différente de celle appliquée à un service

[10] Le critère « des attentes raisonnables en matière de protection de la vie privée » peut être critiqué, notamment dans la mesure où il rend cette protection tributaire de la technologie. De toute façon, les États parties à la Convention européenne des droits de l'homme (CEDH) ne sont pas fondés aujourd'hui à distinguer le trafic empruntant les ondes radio de celui empruntant les câbles (voir, *infra*, la section VI).

[11] Rapport 2007, paragraphe 58.

censé fournir des renseignements sur les menaces pesant sur la sécurité intérieure et ayant (ou ayant eu) un impact plus perceptible sur les droits individuels des ressortissants ou des résidents. Ainsi, des services ne s'étant guère préoccupés jusqu'à présent de la manière dont leur travail affecte les droits individuels (y compris ceux de ressortissants étrangers) doivent désormais commencer à réfléchir à ces questions. Contrairement à l'évolution technologique, l'instauration d'une culture organisationnelle « respectueuse des droits » est un processus relativement lent.

53. Sixièmement, depuis les attaques terroristes du 11 septembre 2001, les budgets et les ressources humaines de bon nombre de services de renseignement ont considérablement augmenté. Comme indiqué dans le rapport de 2007[12], un renforcement aussi rapide comporte divers risques. La tendance naturelle des services de renseignement à collecter trop d'informations est parfois insuffisamment contenue, notamment lorsque les pressions politiques prennent le pas sur l'intégrité et le professionnalisme du personnel, c'est-à-dire les deux qualités incitant le plus souvent les intéressés à s'opposer à une collecte excessive.

54. Enfin, le ROEM constitue dans une large mesure un réseau coopératif international, dont la surveillance pose par conséquent des problèmes spécifiques (voir, *infra*, la section V.E). Pourtant, il convient de signaler sur ce point que les allégations d'absence de contrôle du renseignement d'origine électromagnétique ont également attiré l'attention sur les échanges de renseignements. Même si les données transférées sont censées être couvertes par des normes nationales équivalentes en matière de protection de la vie privée, « la sécurité nationale » constitue habituellement une exception auxdites normes. Il n'est donc pas impossible que, en cas de transfert de données, un service de renseignement ou de sécurité intérieur ne soit pas tenu de se conformer aux règles – relatives à la protection des données – de l'État ayant communiqué les informations.

C. Surveillance massive ?

55. Si l'on garde ces considérations à l'esprit, il est incontestablement opportun d'organiser une discussion appropriée sur le contrôle de la surveillance stratégique et plusieurs États ont déjà pris des initiatives en ce sens. La question revêt une acuité particulière depuis les allégations détaillées d'un ex-consultant de la NSA, Edward Snowden, en juin 2013. Ces allégations ont fait naître des craintes concernant non seulement les activités de cette agence spécifique, mais également le fait que plusieurs de ses homologues étrangers, y compris ceux d'États membres du Conseil de l'Europe, procèdent à « une surveillance massive ». Les craintes soulevées par ces allégations concernant les capacités et les pratiques de la NSA ont été exacerbées par le fait que les entreprises américaines dominent internet et qu'une bonne partie du trafic de cette autoroute de l'information est acheminée via une « dorsale » située en territoire américain. Elles ont notamment conduit l'Assemblée générale des Nations Unies à adopter une résolution sur le droit à la vie privée à l'ère du numérique[13], le Parlement européen à prier sa commission des libertés de procéder à une enquête[14] et l'Assemblée parlementaire du Conseil de l'Europe[15] à prendre position sur des

[12] Rapport 2007, paragraphe 64.

[13] Résolution 68/167 de l'Assemblée générale, « Le droit à la vie privée à l'ère du numérique », 18 décembre 2013. Voir aussi le rapport du Haut-Commissariat des Nations Unies aux droits de l'homme intitulé « Le droit à la vie privée à l'ère du numérique », A/HRC/27/37, 30 juin 2014.

[14] Parlement européen, LIBE, « Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures » (2013/2188(INI)), 21 février 2014.

[15] ACPE, commission des questions juridiques et des droits de l'homme, « Surveillance massive », rapporteur : M. Pieter Omtzigt (avril 2015).

propositions – émanant de fournisseurs de services[16] et d'une coalition d'ONG[17] – en faveur de principes mondiaux de régulation.

56. La surveillance massive n'est pas une notion juridique. Elle peut se définir par opposition à la surveillance « ciblée » telle qu'elle est décrite *supra*. D'aucuns associent ce terme à la pratique d'États policiers tels que l'Allemagne nazie ou à la surveillance envahissante – par la police secrète de l'Union soviétique et des pays d'Europe de l'Est à l'époque du Pacte de Varsovie – de l'ensemble ou d'une grande partie de la population.

57. D'aucuns font valoir, dans le cadre d'un élargissement des perspectives, que la surveillance stratégique n'est qu'un des aspects d'une tendance générale à une surveillance plus proactive de la population, laquelle se traduit par la collecte de données relatives à un large segment de population, données qui seront conservées pendant plusieurs années et disponibles dans le cadre de recherches. Parmi les autres exemples du même type figurent les exigences légales pesant sur les entreprises en matière de conservation et de mise à la disposition de données – sur les passagers des compagnies aériennes, sur les communications téléphoniques et sur les transactions financières – ainsi que de métadonnées internet.

58. L'interception de données en vrac dans les transmissions ou l'obligation pour les entreprises de télécommunication de conserver et de fournir des données de contenu ou des métadonnées aux autorités répressives ou aux services de sécurité s'analysent en une ingérence dans la vie privée et d'autres droits individuels d'une large portion de la population mondiale, en raison du nombre élevé de personnes utilisant des télécommunications de nos jours[18]. En raison de la modification concomitante du comportement social, du moins dans le monde développé, à savoir que les gens exposent une bonne partie de leur vie privée sur les réseaux sociaux et mettent rarement leur téléphone mobile hors tension, ces données peuvent fournir beaucoup plus d'informations touchant à la vie privée que les métadonnées qui consistaient en de simples listes d'appels passés sur le réseau fixe et précisant la durée de chaque communication[19]. Le seul fait pour une personne de savoir que sa conduite en ligne est enregistrée et pourra être ensuite examinée par les autorités répressives peut affecter (et affecte) sa conduite.

59. En ce qui concerne l'utilisation des métadonnées au sein de l'UE, la Cour de justice de l'Union européenne (CJUE), reconnaissant l'impact accru de cette pratique sur les droits individuels et notamment sur la protection de la vie privée, a récemment annulé la directive de l'Union relative à la conservation des données[20]. Les tribunaux des États membres ont donné suite à l'arrêt et souligné la nécessité d'un contrôle amélioré de la collecte des

---

[16] « Global Government Surveillance Reform : The Principles », 9 décembre 2013, www.reformgovernmentsurveillance.com .

[17] « Principes internationaux sur l'application des droits de l'homme à la surveillance des communications », version finale mai 2014, https://en.necessaryandproportionate.org/text.

[18] Voir le quatrième rapport annuel du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 23 septembre 2014, A/69/397, paragraphes 18 et 19 ; voir aussi : Commissaire aux droits de l'homme du Conseil de l'Europe, article du Carnet des droits de l'homme, 24 octobre 2013.

[19] Voir K. Opsahl, « Why Metadata Matters », Electronic Frontier Foundation : www.eff.org/deeplinks/2013/06/why-metadata-matters, et un article de D. Tokmetzis paru initialement dans le journal néerlandais *De Correspondent* : www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/. Voir également la Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux, adoptée le 11 juin 2013 lors de la 1173e réunion des Délégués des Ministres : https://wcd.coe.int/ViewDoc.jsp?id=2074317.

[20] Affaires jointes C-293/12 et C-594/12 : *Digital Rights Ireland et Seitlinger et autres*, 8 avril 2014.

métadonnées[21]. Les exigences en matière de conservation/transfert des métadonnées peuvent également gêner l'exercice de la liberté d'expression et d'association, ainsi que la libre recherche d'informations, tous droits garantis par la Constitution[22].

60. Toutefois, au moins dans une perspective européenne, les principales ingérences concernent la vie privée et la protection des données à caractère personnel[23] et se produisent lorsque les autorités répressives ou bien les services de sécurité et de renseignement peuvent avoir accès d'une manière ou d'une autre aux données en question et les soumettre à un traitement (soit directement, soit par le biais des entreprises de télécommunication agissant pour leur compte).

61. Cela dit, les deux ingérences sont manifestement liées : l'exigence de conservation/transfert crée un risque potentiel de surveillance massive qui se concrétisera dès lors que les critères d'accès aux données sont laxistes et que l'accès aux données à caractère personnel d'un grand nombre d'individus devient par conséquent possible. Ce principe prévaut, quels que soient le ou les services bénéficiant d'un accès. Les métadonnées, en particulier, peuvent faire l'objet d'un traitement automatisé, ce qui explique leur valeur aux yeux des autorités répressives et des services de sécurité intérieure.

62. Comparé aux autorités répressives ou aux services de sécurité intérieure, le ROEM dispose généralement d'un matériel informatique beaucoup plus puissant et jouit donc de la capacité de traiter et d'analyser de grandes quantités de données. Il est donc plus à même de procéder à « une surveillance massive ».

63. La question de savoir si, en fait, les services de ROEM collectent des renseignements sur un grand nombre de personnes fait l'objet d'un débat. Selon l'édition 2013 du rapport de transparence publié par la Direction du renseignement national (Office of the Director of National Intelligence ou ODNI), 90 000 personnes physiques ou morales étrangères auraient été ciblées cette même année en vertu de l'article 702 du FISA[24]. Ce nombre de cibles, comparé aux quelque 3 milliards de personnes utilisant régulièrement internet et les systèmes de télécommunication, ne saurait justifier l'emploi à bon escient du terme « surveillance massive ». Toutefois, il convient également de tenir compte du fait que, premièrement, le mot « personnes morales » implique en fait le ciblage d'un nombre beaucoup plus important de personnes physiques ; deuxièmement, les cibles elles-mêmes communiquent avec d'autres personnes ; troisièmement, le taux d'erreur aboutit à la collecte de communications de personnes autres que les cibles directes. Un facteur d'erreur (au demeurant modeste) de 9 entraînerait l'interception, la conservation et le traitement d'au moins 810 000 communications privées[25]. Même si la minimisation diligente des données primaires par des analystes en chair et en os permet généralement d'éliminer une partie des erreurs manifestes, ce processus ne saurait être totalement exhaustif et on ne saurait non

[21] Voir également la décision G 47/2012 et d'autres rendues le 27 juin 2014 par la Cour constitutionnelle autrichienne. Dans certaines affaires, des juridictions nationales ont précédé la CJUE dans la décision de déclarer incompatible une partie des dispositions ; voir notamment l'arrêt rendu par la Cour constitutionnelle fédérale allemande (Bundesverfassungsgericht) dans 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 concernant la Directive relative à la conservation des données.

[22] Voir, *infra*, la section VI.

[23] La relation entre vie privée et protection des données n'est pas analysée dans le cadre de la présente étude. Ces deux droits individuels sont considérés comme distincts dans la Charte des droits fondamentaux de l'UE et comme deux éléments différents d'un même droit dans l'article 8 de la CEDH.

[24] Voir http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013. Voir également www.washingtonpost.com/world/national-security/us-releases-data-on-sensitive-surveillance-programs-for-first-time/2014/06/27/46bbd47e-fe3a-11e3-8176-f2c941cf35f1_story.html.

[25] B. Gellman, J. Tate, A. Soltan, « In NSA-intercepted data, those not targeted far outnumber the foreigners who are », *The Washington Post*, 5 juillet 2014.

plus tenir pour acquis que cette minimisation est toujours menée avec la diligence requise, du moins en ce qui concerne les étrangers (dans la mesure où le processus n'est pas systématiquement défini comme une tâche prioritaire au sein du service)[26]. Il convient d'avoir à l'esprit que les États-Unis assument des responsabilités au niveau mondial en matière de sécurité et, par conséquent, sont tenus de collecter des renseignements sur l'ensemble de la planète. Même en tenant compte de ce facteur, il semble évident que la NSA collecte et, même après minimisation, conserve des données concernant un très grand nombre de personnes.

64. La question essentielle, cependant, n'est pas de déterminer si cette pratique et les mesures équivalentes prises par d'autres services de ROEM constituent une « surveillance massive »[27] – des termes qui, de toute façon, ne correspondent à aucune notion juridique –, mais de décider comment il convient de contrôler convenablement la surveillance stratégique dans un État de droit.

IV. Juridiction

65. La surveillance stratégique peut être exercée à la fois sur le territoire et hors du territoire d'un État par des unités opérant depuis une base militaire située dans un pays allié, une ambassade, ou bien un navire ou un aéronef évoluant dans les eaux internationales ou dans l'espace aérien international. La collecte de renseignements depuis la haute mer ou depuis le territoire d'un État tiers consentant n'est pas contraire à la norme de droit international coutumier de non-intervention[28]. Toutefois, la jurisprudence de la Cour européenne des droits de l'homme et du Comité des droits de l'homme des Nations Unies précise que les obligations inhérentes à la protection des droits de l'homme peuvent s'étendre à des activités menées entièrement hors du territoire national[29]. L'équipement de collecte installé

[26] Voir B. Gellman, « How 160,000 intercepted communications led to our latest NSA story », www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html.

[27] Le rapport du Conseil national de la recherche des États-Unis utilise à la place les termes de collecte « en vrac » et « ciblée ». Soulignons qu'il est faux d'affirmer que toute collecte réalisée à l'aide de sélecteurs est ciblée puisque le recours à un sélecteur large (comme « Syrie ») générera une grande quantité de données. Selon les auteurs dudit rapport, ce n'est pas tant la quantité de données qui confère à la collecte son caractère « en vrac », mais le fait qu'elle permet d'obtenir une proportion plus importante de données supplémentaires en plus de celles visant les cibles connues au moment du lancement du processus : « Rapport du Conseil national de la recherche des États-Unis », p. 33.

[28] Reste la question de la preuve. Dans *Weber et Saravia c. Allemagne*, Requête n° 54934/00, décision du 29 juin 2006, les requérants avançaient qu'en interceptant leurs télécommunications privées commençant et finissant dans un pays tiers, les autorités allemandes avaient violé le droit international. La Cour a considéré que le terme « loi » fait référence au droit national, y compris les règles du droit international applicables dans l'État considéré. Toutefois, elle a exigé « qu'il soit démontré devant elle, par des indices concordants, que les autorités de l'État défendeur ont procédé à l'étranger à des activités contraires à la souveraineté de l'État étranger, donc au droit international » (paragraphe 87). Les juges de Strasbourg ont conclu qu'en l'espèce les requérants n'étaient pas parvenus à prouver leurs allégations.

[29] En ce qui concerne la Cour européenne des droits de l'homme, voir les arrêts *Ilaşcu et autres c. République de Moldova et Russie, Requête* n° No. 48787/99 (8 juillet 2004), *Öcalan c. Turquie, Requête* n° 46221/99 (12 mai 2005), *Al-Saadoon et Mufdhi c. Royaume-Uni, Requête* n° 61498/08 (2 mars 2010) et *Al-Jedda c. Royaume-Uni, Requête* n° 27021/08 (7 juillet 2011), Hassan c. *Royaume-Uni*, *Requête* n° 29750/09, 16 septembre 2014, Jaloud c. Pays Bas, *Requête* n° 47708/08, 20 novembre 2014. En 2014, le Comité des droits de l'homme des Nations Unies a déclaré : « L'État partie devrait : *a*. prendre toutes les mesures nécessaires pour garantir que ses activités de surveillance, à l'intérieur et à l'extérieur de son territoire, soient conformes aux obligations découlant du pacte, notamment de l'article 17 ; en particulier, des mesures devraient être prises pour garantir que toute immixtion dans la vie privée soit faite conformément aux principes de légalité, de proportionnalité et de nécessité, indépendamment de la nationalité des personnes dont les communications sont directement surveillées et de l'endroit où elles se trouvent » (CCPR/C/USA/CO/4, paragraphe 22). Voir aussi : rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 4e rapport annuel, 23 septembre 2014, A/69/397.

dans les bases militaires ou à bord de navires évoluant hors du territoire national peut donc également relever de la « juridiction » des États parties au traité pertinent[30]. En tout cas, le traitement, l'analyse et la distribution de ce matériel sont régis à la fois par le droit national et les obligations internationales en matière de protection des droits de l'homme pesant sur les États[31].

66. Deux remarques supplémentaires s'imposent dans ce contexte. Il peut être techniquement possible à un service situé dans un État (A) d'accéder à distance à des ordinateurs situés physiquement sur le territoire d'un autre État (B), puis d'y implanter un logiciel malveillant afin de pouvoir le surveiller. Cette faculté technique ne change rien au fait que l'ordinateur en cause est situé sur le territoire de B et, à ce titre, relève incontestablement du droit pénal et administratif de cette juridiction[32]. Par conséquent, si A parvient à implanter un logiciel malveillant – aux fins de protection de sa sécurité ou d'enquête pénale – sur des ordinateurs situés en B, il risque par là même de violer la règle de non-intervention, à moins de s'être conformé au droit de B (à supposer que ce dernier autorise pareille pratique).

67. Une autre question connexe découle du fait qu'un État (A) peut imposer des obligations légales à des sociétés – enregistrées en vertu de son droit interne et proposant des services informatiques à des personnes physiques et morales situées dans un État B – afin qu'elles mettent à sa disposition, aux fins d'enquête pénale ou de sécurité nationale, les données générées par la fourniture desdits services. Cette obligation de divulgation peut même être assortie de sanctions pénales en vertu de la législation en vigueur dans A. Il est généralement impossible d'interdire une telle divulgation, dans la mesure où la clause du contrat – passé entre le fournisseur de services et la personne physique ou morale cliente – relative à la préservation du caractère confidentiel des données prévoit généralement une exception en faveur des dispositions contraires éventuelles du droit national. On peut donc arriver dans un tel contexte à un conflit entre la législation de A et le droit interne de B visant à protéger les données (et prévoyant éventuellement des sanctions pénales en cas de violation). Le marché de la fourniture de services internet étant dominé par des entreprises américaines (comme Microsoft, Apple, Google, Facebook ou Twitter), les obligations imposées par la législation des États-Unis en matière de divulgation revêtent une importance particulière. En tout cas, le risque que des entreprises soient soumises à des obligations concurrentes, voire antagonistes, justifie les tentatives de définition de normes internationales minimales en matière de protection de la vie privée.

V. Contrôle : contextes constitutionnel et organisationnel

A. Organisation

68. Comme indiqué dans le rapport de 2007, les États divergent quant à l'organisation de leurs fonctions de sécurité. Il s'agit là d'un point important à prendre en considération dans le contexte du contrôle, dans la mesure où toute mesure pertinente se doit de tenir compte des modalités d'organisation des fonctions en jeu. Même si le coût de la conservation des données et de la largeur de bande diminue rapidement, le ROEM demeure une activité

[30] Voir l'avis de la Commission de Venise n° 363/2005 sur les obligations légales internationales des États membres du Conseil de l'Europe concernant les lieux de détention secrets et le transport interétatique des prisonniers, tel qu'il a été adopté lors de la 66e session plénière (Venise, 17-18 mars 2006). Voir également les arrêts rendus par la Cour dans les affaires *Medvedyev et autres c. France* (29 mars 2010) et *Hirsi Jamaa et autres c. Italie* (23 février 2012).

[31] Dans *Weber et Saravia*, la Cour avait conclu que « [d]es signaux émis depuis des pays étrangers étaient surveillés par des sites d'interception situés sur le sol allemand et les données recueillies étaient utilisées en Allemagne » (paragraphe 88).

[32] Voir la Convention sur la cybercriminalité, 2001, STCE n° 185, articles 2 à 6 et 22.

onéreuse qui exige des compétences techniques pointues. Il a déjà été rappelé *supra* que bon nombre d'États ne disposent pas de ces compétences ou ne sont pas désireux de supporter les coûts correspondants. Tous les États développés sont contraints de nos jours d'assumer la fonction défensive de cyber-sécurité. En ce qui concerne les États disposant d'une capacité ROEM offensive, certains ont opté pour la création d'un service spécialisé dans le renseignement d'origine électromagnétique (c'est le cas, par exemple, des États-Unis, du Royaume-Uni et de la Suède), tandis que d'autres confient cette tâche au service de renseignement extérieur (Allemagne, France). Aux Pays-Bas, les services de renseignement et de sécurité civile et militaire ont créé une structure conjointe appelée Unité commune de renseignements d'origine électromagnétique de cyberdéfense.

B. Forme du mandat

69. La plupart des États démocratiques, conscients de l'impact de la surveillance stratégique sur les droits individuels, ont défini au moins une partie de la fonction de ROEM dans la législation primaire[33]. Comme expliqué *infra* dans la section VI, cet énoncé du mandat du service compétent correspond également à une exigence posée par la jurisprudence de la CEDH. Des normes ou des lignes directrices plus détaillées sont aussi, en règle générale, définies dans des textes promulgués par l'exécutif (le plus souvent sous forme de décrets d'application rendus publics) ou diffusés par directeur du service concerné dans des circulaires (le plus souvent confidentielles). Le caractère technique de la question et la coopération internationale dans le cadre de laquelle les données en vrac sont transférées entre services de ROEM peuvent poser certains problèmes sous l'angle de la qualité de la loi (prévisibilité, etc.). Cette carence est notamment apparue à l'occasion de l'examen en 2008, par la Cour européenne des droits de l'homme, du mandat du service de ROEM britannique (le GCHQ) et de l'évaluation en 2014 du même mandat par le tribunal britannique chargé de juger les abus de pouvoir en matière d'enquête (IPT) (voir, *infra*, la section VI).

C. Priorités en matière de sécurité/contenu du mandat

70. Il existe un lien étroit entre la manière plus ou moins précise dont le mandat du service est défini et le risque d'abus. Le mandat du service de ROEM détermine l'essentiel des tâches confiées à l'organe ou aux organes de contrôle et/ou de supervision externe, ce qui justifie l'attention apportée à cette question dans le cadre du présent rapport. Lorsque le mandat d'un service de ROEM est défini de manière suffisamment large pour autoriser la collecte de données « pertinentes », « relatives à des services de renseignement étrangers » ou « présentant un intérêt » au regard d'enquêtes antiterroristes, le service compétent a toutes les chances de procéder à une collecte excessive (rapport de 2007, paragraphe 58). Le Conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board ou PCLOB) des États-Unis a estimé que la NSA avait collecté, en toute légalité, de très grosses quantités de renseignements extérieurs en vertu du programme de l'article 702 (voir, *infra*, le paragraphe 118). Toutefois, la documentation justifiant cette collecte est souvent lacunaire, l'agence s'étant contentée de démontrer le caractère étranger de la cible sans expliquer en quoi la collecte de renseignements la concernant pourrait renforcer la sécurité nationale des États-Unis[34]. Une conclusion

[33] Voir, par exemple, la loi suédoise sur le renseignement militaire (2000:133), la loi allemande sur le renseignement d'origine électromagnétique (2008:717) souvent désignée par l'abréviation « loi G10 ») et la loi du Royaume-Uni de 2000 sur la réglementation des pouvoirs d'enquête (RIPA).

[34] Conseil de surveillance de la vie privée et des libertés civiles (PCLOB [Privacy and Civil Liberties Oversight Board], États-Unis), « Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act » (Rapport sur le programme de surveillance exécuté en vertu de l'article 702 de la loi relative à la surveillance du renseignement étranger), 2 juillet 2014 (ci-après « le rapport du PCLOB sur l'article 702 »), p. 135 : « l'examen par le Conseil du programme de l'article 702 a révélé que les procédures de documentation des décisions de ciblage au sein de la NSA, ainsi que les procédures de contrôle de ces

analogue a été formulée par l'organe de surveillance néerlandais, la CTIVD[35]. L'expérience acquise aux Pays-Bas révèle que, même lorsque l'organe de contrôle dispose formellement du pouvoir de formuler des avis concernant le caractère proportionnel/approprié d'une opération spécifique de collecte de renseignements (voir, *infra*, la section X), il n'est pas toujours en mesure de l'exercer faute d'une documentation à analyser.

71. Les opérations de ROEM visant à obtenir des renseignements relatifs au terrorisme sont généralement mieux documentées (une enquête pénale ou de sécurité partiellement spécifique a le plus souvent été précédemment ouverte, de sorte qu'il existe déjà une documentation justificative). Toutefois, comme indiqué *infra* dans la section VI, un critère exigeant « que l'information soit pertinente sous l'angle de la lutte antiterroriste » est nettement moins strict qu'un critère exigeant que l'individu surveillé soit impliqué dans un acte terroriste spécifique (ou observe, au moins, une conduite à caractère terroriste s'analysant en une infraction pénale).

72. Une autre question liée au mandat tient à la distinction opérée – principalement aux États-Unis, mais aussi dans d'autres États[36] – entre ressortissants et résidents d'une part et non-ressortissants et non-résidents d'autre part. Cette question est pertinente car une telle distinction peut aboutir à la définition de normes différentes en matière à la fois de critères de ciblage, de conservation, de communication, etc., des données. En raison de la fréquence, dans le village planétaire d'aujourd'hui, des communications entre ressortissants et non-ressortissants d'un État donné, des normes plus laxistes en matière de ciblage et de conservation des communications impliquant au moins un non-ressortissant posent le risque d'abus en créant une échappatoire pouvant justifier la collecte d'informations sur des citoyens qui jouiraient autrement d'une protection en vertu du droit interne. De plus, d'aucuns critiquent cette distinction automatique en invoquant d'autres raisons fondamentales : les droits conférés à la fois par le PIRDCP et la CEDH sont reconnus à toute personne relevant de la juridiction de l'État considéré[37]. Tous les individus jouissent par conséquent d'un droit à la vie privée opposable aux États parties à ces instruments. La réglementation en vigueur aux États-Unis prévoit que tous les individus jouissent d'un droit à la vie privée[38]. De plus, la distinction difficile, déjà évoquée, entre communications

---

décisions au sein de l'exécutif, se concentrent principalement sur la détermination du caractère étranger, c'est-à-dire sur la vérification que les cibles potentielles sont des personnes n'ayant pas la nationalité américaine et dont on peut raisonnablement supposer ne se trouvent pas sur le territoire des États-Unis […] [cette approche] est révélatrice de la catégorie d'informations collectées dans le cadre du renseignement étranger que lesdits services espèrent obtenir en ciblant une personne donnée ; elle permet d'indiquer au moyen d'une simple phrase courte pourquoi l'analyste estime qu'un tel ciblage permettra au service de renseignement extérieur de collecter des informations. En raison de cette pratique, l'équipe de surveillance (composée de fonctionnaires du ministère de la Justice et de la Direction du renseignement national) de l'application de l'article 702 n'est pas en mesure de vérifier les décisions pertinentes du service de renseignement extérieur avec la même rigueur que la qualité de non-ressortissant des États-Unis de la cible ». Le PCLOB a recommandé des améliorations en ce qui concerne la motivation et la documentation des décisions (p. 134) sous la supervision d'un tribunal spécialisé, le Foreign Intelligence Surveillance Court (FISC) (p. 136).

[35] De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) – la Commission de controle des services de renseignements et de securité, « Rapport annuel 2011-2012 », p. 96.

[36] Les garanties mises en place par la législation allemande (voir, *infra*, les paragraphes 112 à 114) ne s'appliquent pas aux non-ressortissants/non-résidents : cette lacune majeure sous l'angle de la protection des droits de l'homme est critiquée par une partie de la doctrine ; voir B. Huber, « Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite », *Neue Juristische Wochenschrift*, 2013, question 35, p. 2572-2576.

[37] Voir les critiques exprimées par 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, 4e rapport annuel, 23 septembre 2014, A/69/397.

[38] Directive présidentielle (*Presidential Decision Directive*) (PPD) no 28, article 4 : « Toute personne doit être traitée avec dignité et respect, quels que soient sa nationalité et l'endroit où elle réside, et voir reconnaître son intérêt légitime à ce que les informations à caractère personnel qui la concerne soient traitées dans le respect de

intérieures et extérieures (voir, *supra*, la section IV) est censée profiter aux non-ressortissants, dans la mesure où elle entraîne normalement l'application en pratique des normes les plus strictes (celles qui protègent les ressortissants) aux processus de minimisation automatisés[39]. À supposer qu'il en soit réellement ainsi, il s'agit d'un pas important dans la bonne direction que les autres États devraient limiter à moins qu'ils ne l'aient déjà fait[40]. Toutefois, cette reconnaissance des droits à la vie privée des étrangers autoriserait malgré tout l'application de critères de pertinence, de proportionnalité et de nécessité aux opérations de ciblage, de conservation, de suppression et de transfert[41]. En tout cas, sans une supervision stricte et indépendante des banques de données (voir, *infra*, la section X), il est impossible de s'assurer que les quantités de données à caractère personnel visant des étrangers ne sont pas excessives (et utilisées de différentes manières).

73. Autoriser la collecte de ROEM pour « le bien-être économique de la nation »[42] peut faire naître des doutes concernant l'utilisation éventuelle des renseignements d'origine électromagnétique à des fins d'espionnage économique ou dans le but de conférer un avantage aux sociétés enregistrées dans un État dans le cadre d'un marché public ou en d'autres circonstances. L'interrelation entre intérêts privés et publics en matière de contrats de défense dans certains États peut renforcer les soupçons de ce type. Il existe au moins trois domaines d'activité commerciale dans lesquels la surveillance stratégique est utile (en dehors du rôle qu'elle peut jouer contre les tentatives d'espionnage économique visant les entreprises du pays concerné) : la prolifération des armes de destruction massive (et, en règle générale, la violation du contrôle des exportations), le contournement de sanctions imposées par les Nations Unies ou l'Union européenne et le blanchiment de capitaux à grande échelle. Lorsque le mandat du service de ROEM est défini en termes vagues, il doit être complété par l'interdiction claire de se livrer à l'espionnage économique, comme c'est actuellement le cas de la réglementation en vigueur aux États-Unis[43], par un contrôle efficace et par la défense pour un ministère ou un organisme administratif chargé de promouvoir le commerce de confier une mission au dit service.

---

sa vie privée ». Cette disposition ne change en rien la position officielle des États-Unis à savoir que le PIRDCP n'a pas d'effet extraterritorial.

[39] Rapport du PCLOB sur l'article 702, p. 100 : « En pratique, les personnes n'étant pas des ressortissants américains bénéficient également des restrictions à l'accès et à la conservation imposée par les procédures de minimisation et/ou de ciblage des différents services. Bien que n'étant légalement imposées qu'en ce qui concerne les citoyens américains, lesdites procédures sont en fait appliquées à l'ensemble des cibles, dans la mesure où il s'avère trop onéreux et trop compliqué d'identifier et de retirer les informations visant des ressortissants des États-Unis en présence d'un gros volume de données. »

[40] C'est notamment le cas de la Suède où la loi pertinente (loi 2008:717 relative aux renseignements d'origine électromagnétique) énonce à la fois une obligation de minimisation par le biais de sélecteurs (article 5) et une obligation de destruction (articles 3 et 7). Cette garantie n'est pas explicitement limitée aux seuls ressortissants suédois.

[41] Voir, par exemple, l'article 7 de l'ordonnance suédoise 2008:261 qui interdit la communication de renseignements à des services étrangers dès lors qu'une telle opération porterait atteinte à des intérêts suédois, de sorte qu'il est plus facile de transférer des renseignements visant des non-ressortissants ou des non-résidents.

[42] Voir, par exemple, l'article 5(3) de la loi sur la réglementation des pouvoirs d'enquête britannique (*Regulation of Investigatory Powers Act* [2000] ou RIPA), même si l'article 5(5) du même instrument prévoit que l'information recherchée doit viser « des actes ou des intentions commis/nourries par des personnes situées hors des îles britanniques ».

[43] PPD n° 28, article 2 : « Les renseignements d'origine électromagnétique collectés en vrac ne pourront en aucun cas être utilisés dans le but de […] conférer un avantage compétitif à des entreprises ou à des secteurs d'activité commerciale américains. » Une note de bas de page précise : « La poursuite de certains objectifs économiques, comme l'identification de violation des règles du commerce ou d'un régime de sanctions ou bien l'influence ou l'emprise d'un gouvernement, ne sera pas considérée comme visant à conférer un avantage compétitif. »

74. Une question particulière, compte tenu de la coopération étroite qui existerait entre les services de ROEM des pays occidentaux, tient au risque de contournement des procédures de surveillance nationales plus strictes. Chaque État a tendance à prévoir que, lorsque les deux participants à une télécommunication relèvent de sa juridiction, cet échange peut être qualifié de communication intérieure, même si la liaison ou une partie de celle-ci franchit d'une manière ou d'une autre les limites du territoire national. Les systèmes automatisés éliminent ces communications intérieures mais tolèrent un taux d'erreur (ce qui paraît inévitable si l'on désire se prémunir contre l'effacement accidentel de certaines communications extérieures). Cette approche ne résout que partiellement le problème. Comme noté *supra*, le risque existe de voir le service du pays X demander à son homologue du pays Y de collecter des renseignements sur un ressortissant ou un résident de X et d'éviter ainsi de violer toute limitation légale à laquelle il pourrait être soumis en ce qui concerne les opérations de renseignement intérieur. Ce problème peut être partiellement résolu en adoptant une législation interdisant au service du pays X de recourir activement à des homologues de nations amies pour collecter des renseignements sur ses propres ressortissants ou résidents. On peut également affirmer que, dans ce domaine, la rivalité entre institutions pourrait renforcer le respect d'une telle limitation : le service responsable de la sécurité intérieure dans X a (ou devrait avoir) le monopole des opérations de collecte de renseignements sur le territoire national. Il est probable qu'il veillerait alors jalousement à conserver ce monopole[44]. Cela dit, l'argument de la rivalité institutionnelle, à supposer qu'il soit pertinent, ne vaut que pour les services d'un même pays. Dès lors qu'un service de ROEM très puissant propose des renseignements utiles aux services de sécurité intérieure de X, il est très peu probable que ce dernier refuse. Le même service de X fera tout pour s'opposer à l'interdiction de réception passive de tels renseignements (et la ligne de séparation entre réception active et passive est loin d'être aussi nette que certains pourraient le croire, dès lors que les services en question ont « rapproché leurs points de vue » dans le cadre d'une coopération très ancienne). En outre, comme indiqué *supra*, il arrive que le transfert porte sur des données en vrac : une pratique logique du point de vue de l'efficacité (utilisation optimale des capacités non exploitées, des ressources en traduction et autres compétences), mais présentant également le risque d'un contournement des règles en matière de collecte de renseignements au niveau national. L'une des garanties appropriées dans les deux cas consiste à prévoir que le matériel en vrac transféré ne pourra faire l'objet de recherches que si toutes les exigences applicables au traitement national des données sont remplies et si l'opération est dûment autorisée en vertu de la même procédure que celle observée par le service de ROEM de l'État de destination en vertu de ses propres règles[45].

75. Parmi les limitations relevant de « la politique étrangère » pouvant être mentionnées dans ce contexte figure l'engagement de ne pas transférer de renseignements de nature à permettre à un pays de museler des militants de la liberté de parole ou de la démocratie. Les États-Unis ont passé des accords d'échange de renseignements avec un grand nombre de pays, dont certains dotés d'un gouvernement autocratique, et une limitation de ce type figure dans la PPD (Presidential Policy Directive) n° 28[46].

---

[44] Ainsi, en vertu de l'article 4 de la loi suédoise sur le renseignement militaire, le service de ROEM ne peut pas participer à des enquêtes pénales. Cette interdiction est interprétée comme signifiant que les opérations dirigées par ledit service et le recours à des sélecteurs associés à un individu donné doivent cesser dès lors qu'une enquête pénale est ouverte contre l'intéressé et que des mesures de surveillance (prévues et limitées par le Code de procédure judiciaire) lui sont appliquées (Prop. 2006/07, 63, p. 108).

[45] Voir, *infra*, dans la section VI, l'analyse de l'affaire *Liberty (The National Council For Civil Liberties) v. GCHQ, SIS, the Security Service*, tribunal britannique chargé de juger les abus de pouvoir en matière d'enquête (IPT), [2014] UKIPTTrib 13_77-H, arrêt et ordonnance, [2015] UKIPTTrib 13_77-H.

[46] Article 2 : « Les renseignements d'origine électromagnétique collectés en vrac ne pourront en aucun cas servir à faire cesser ou à étouffer des critiques ou des contestations, pas plus qu'à désavantager des personnes sur la base de leur origine ethnique, de leur race, de leur genre, de leur orientation sexuelle ou de leur religion. »

76. En conclusion sur le mandat, deux exemples peuvent être cités. En vertu de l'article 5(3) de la loi de 2000 du Royaume-Uni sur la réglementation des pouvoirs d'enquête (RIPA), un mandat peut être délivré : *a*. dans l'intérêt de la sécurité nationale ; *b.* dans le but de prévenir ou de détecter une infraction grave ; *c.* dans le but de protéger le bien-être économique du Royaume-Uni ; ou *d*. dans le but, en présence de circonstances jugées par le secrétaire d'État comme équivalant à celles dans lesquelles il délivrerait un mandat en vertu du paragraphe *b*, de conférer un effet aux dispositions d'un quelconque accord international d'entraide judiciaire. Malgré la présence de dispositions limitant encore plus la manière dont les renseignements peuvent être collectés, les objectifs fondamentaux de la loi sont exprimés en termes très généraux[47].

77. En vertu de l'article 1 de la loi suédoise sur les ROEM (2008 :717), section 1 (traduction assurée par le rapporteur):

> « Dans le cadre du renseignement militaire, les ROEM ne peuvent être utilisés que pour identifier : 1. des menaces militaires extérieures pesant sur le pays ; 2. les conditions de la participation suédoise aux opérations de soutien de la paix et d'aide humanitaire ou les menaces sécuritaires pesant sur des intérêts suédois dans le cadre du déploiement de tels efforts ; 3. des questions stratégiques – relevant du terrorisme international et d'autres formes graves de criminalité transnationale – susceptibles de faire peser une menace sur des intérêts nationaux essentiels ; 4. la mise au point et la prolifération d'armes, de matériel et de produits militaires énumérés dans la loi 2000:1064 sur le contrôle des produits à double usage ; 5. les graves menaces pesant sur des infrastructures publiques ; 6. les conflits se déroulant à l'étranger et pouvant avoir des implications pour la sécurité internationale ; 7. les opérations de services de renseignement étrangers visant à porter atteinte à des intérêts suédois ; ou 8. les actes ou les intentions d'une puissance étrangère revêtant une importance particulière pour les politiques étrangères, de sécurité et de défense de la Suède. »

78. Le même article contient également une disposition visant à tenir compte du fait que le service de ROEM a besoin de procéder constamment à des tests et que cette pratique peut, elle aussi, influer sur l'exercice de droits individuels : « Si cela s'avère nécessaire pour le renseignement militaire, celui-ci peut également collecter des renseignements d'origine électromagnétique au moyen d'une interception dans le but : 1. de suivre les changements intervenant dans ce domaine à l'étranger, les progrès de la technologie et les méthodes de protection des signaux ; et 2. d'améliorer constamment la technologie et la méthodologie requises pour mener les activités prévues dans la présente loi. » Les tests sont, eux aussi, soumis à un régime d'autorisation juridictionnel (voir, *infra*, le paragraphe 118)[48].

79. La Commission de Venise a déjà exprimé l'avis selon lequel « il est absolument essentiel » que les normes relatives aux services de sécurité intérieure soient aussi claires et concises que possible, afin que les tâches que ces services peuvent entreprendre légalement soient définies clairement et que les normes leur étant applicables ne soient

[47] Voir la PPD n° 28 et l'article pertinent de la loi sur la surveillance du service de renseignement extérieur (*Foreign Intelligence Surveillance Act*), Pub. L. n° 95-511, 92 Stat. 1783 (codifié sous sa version modifiée dans 50 USC : paragraphes 1801 à 1885c) ; ledit article 50 USC, paragraphe 1881a(a) (voir la note de bas de page 114) dresse une liste de motifs légitimes qui, dans l'ensemble, est beaucoup plus restrictive.

[48] Les renseignements obtenus sur la base des tests peuvent être conservés dans le but de faciliter la conception d'opérations futures, mais ne peuvent pas être communiqués au commanditaire ou à tout autre organe, PROP 2006/07:63, p. 109.

gardées secrètes que dans la mesure strictement nécessaire[49]. Il en va de même pour le ROEM.

D. Contrôle et attribution de tâches par le gouvernement

80. Comme nous l'avons déjà indiqué *supra*, le ROEM peut servir à obtenir des renseignements d'ordre diplomatique, économique, militaire et domestique. En ce qui concerne la première catégorie, l'entité chargée d'attribuer les tâches est généralement le gouvernement lui-même. Il en va de même en ce qui concerne la deuxième catégorie, même si, dans ce contexte, certains organes de l'administration publique comme les douanes peuvent également intervenir. Les forces armées, le renseignement militaire, etc., sont les entités chargées d'attribuer les tâches dans le cadre de la troisième catégorie. En ce qui concerne la quatrième catégorie, le facteur important tient au lien éventuel avec l'enquête menée pour infraction touchant la sécurité.

81. On peut distinguer plusieurs variantes. Le droit interne peut autoriser un organe de sécurité intérieure ou la police à « attribuer une tâche » au service de ROEM soit uniquement dans le but de collecter des renseignements « stratégiques » (comme c'est déjà le cas, par exemple, en Suède), soit dans ce but ainsi que dans le cadre d'une opération de collecte de renseignements visant des individus ou des groupes liés à des infractions spécifiques touchant la sécurité (comme c'est le cas notamment aux États-Unis). Il est possible de concevoir un système totalement différent dans lequel aucune instance ne jouit du pouvoir d'attribuer une tâche, mais où le service de renseignement a la possibilité ou le devoir de transférer les renseignements faisant état de la commission d'une infraction touchant la sécurité, ou relevant de la criminalité organisée au service de police ou à l'organe de sécurité intérieure compétent pour enquêter sur de tels agissements.

82. Dans tous les cas, une supervision s'impose, laquelle doit être adaptée à chaque type de fonction.

83. Les organes chargés d'attribuer les tâches doivent avoir conscience que, vu leur qualité de consommateur des renseignements qu'ils réclament, ils ne sauraient être perçus comme exerçant un contrôle externe sur le processus de collecte desdits renseignements (rapport de 2007, paragraphe 112).

E. Contrôle du réseau

84. En raison de sa situation géographique spécifique, un État peut avoir accès à différentes télécommunications par câble ou par satellite et donc collecter des données présentant un intérêt pour d'autres pays. De plus, internet repose sur la fragmentation des communications en « paquets » acheminés selon divers itinéraires puis « réassemblés », de sorte que plusieurs États peuvent avoir accès chacun à différentes parties du même message. Par conséquent, alors que bon nombre d'États coopèrent en échangeant des renseignements intérieurs et extérieurs (parfois sur la base d'une obligation énoncée dans un traité), les liens entre États alliés en ce qui concerne le ROEM peuvent être encore plus forts. Certains pays ont ainsi conclu des arrangements permanents en matière de coopération et mis en place des liens organisationnels étroits entre leurs services de ROEM respectifs. La règle dite « de la maîtrise de l'information par son auteur » (en vertu de laquelle l'utilisation de renseignements transférés par un service à un autre est soumise à l'autorisation du premier) peut donc constituer un obstacle encore plus important à la supervision.

[49] Voir la page 7 du document CDL-INF(98)6 de la Commission de Venise, ainsi que les paragraphes 25 et 227 du rapport de 2007.

VI. Contrôle des activités de sécurité et jurisprudence de la Cour européenne des droits de l'homme

A. La Cour européenne des droits de l'homme et la surveillance stratégique en général

85. Pour commencer, il convient de se rappeler que la CEDH énonce des normes minimales. Ainsi, la jurisprudence de la Cour européenne des droits de l'homme ne constitue qu'un point de départ pour les États européens. De toute évidence, les normes élaborées par la Cour ne s'appliquent ni aux États-Unis ni aux autres États n'étant pas parties à cet instrument.

86. Dans sa jurisprudence relative aux mesures secrètes de surveillance, la Cour a énoncé des garanties minimales devant être reprises dans la législation en vue d'éviter les abus de pouvoir : définition de la nature des infractions pouvant donner lieu à une ordonnance d'interception ; définition des catégories de personnes pouvant voir leur ligne téléphonique mise sur écoute ; procédure à suivre afin d'examiner, d'utiliser et de conserver les données obtenues ; précautions à prendre en cas de communication des données à d'autres parties ; circonstances dans lesquelles des enregistrements peuvent ou doivent être effacés ou des bandes détruites[50]. Il convient de souligner que plusieurs de ces normes (telles qu'elles sont décrites dans la sous-section qui suit) devraient être adaptées pour pouvoir s'appliquer à la surveillance stratégique.

87. La Cour n'a jusqu'à présent examiné que deux affaires visant la surveillance stratégique : *Weber et Saravia c. Allemagne* et *Liberty et autres c. Royaume-Uni*[51]. Cette dernière portait uniquement sur les termes « prévue par la loi ». La première a donné lieu à une décision de recevabilité présentant toutefois la particularité d'être moins détaillée et moins motivée que les arrêts habituellement rendus par les juges de Strasbourg. Toutefois, les questions relatives au caractère « nécessaire dans une société démocratique » et à la proportionnalité des mesures, ainsi que des recours n'ont encore jamais fait l'objet d'un examen minutieux par la Cour dans le contexte de la surveillance stratégique. De même, on ne saurait prétendre que les normes fixées dans l'arrêt *Weber et Saravia* – qui porte sur le modèle allemand – sont nécessairement applicables dans leur intégralité à des systèmes de droit interne reposant sur une législation construite différemment[52]. Affirmer que la jurisprudence de la Cour est limitée ne revient pas à dire que la jurisprudence des tribunaux nationaux portant sur la CEDH est maigre : l'organe de supervision néerlandais, la CTIVD, et l'IPT britannique ont discuté de l'application des normes de la Convention à leurs droits nationaux respectifs, une question également traitée dans la suite du présent rapport.

88. Le premier point qu'il convient de noter est que « la sécurité nationale » ne se limite pas aux enquêtes visant des infractions – touchant la sécurité – consommées, en cours ou en préparation[53]. La formulation de l'article 8 permet expressément les ingérences dans la vie privée au nom de la sécurité nationale, du bien-être économique du pays, de la sûreté

[50] Voir notamment l'arrêt *Weber et Saravia c. Allemagne* précité, paragraphe 95.

[51] *Liberty et autres c. Royaume-Uni*, Requête n° 58243/00, 1er juillet 2008.

[52] La Cour a notamment remarqué, parmi les garde-fous de nature à renforcer le contrôle, la mesure consistant à marquer les renseignements obtenus dans le cadre d'opérations de ROEM, sous peine de compliquer la tâche de l'organe de contrôle au cas où lesdits renseignements seraient fusionnés avec d'autres informations obtenues par le Service fédéral de renseignement (Bundesnachrichtendienst) (BND). Ce garde-fou est superflu dès lors que la base de données se compose uniquement de renseignements d'origine électromagnétique, à condition toutefois que seul le service de ROEM puisse y avoir accès.

[53] *Weber et Saravia c. Allemagne*, paragraphe 104.

publique ou bien de la prévention des désordres ou des crimes. La collecte par des services étrangers de renseignement n'étant pas liée (ou directement liée) à des infractions pénales, elle peut donc relever de l'un ou plusieurs des cas de figure susmentionnés. Comme indiqué *supra*, le fait qu'un traité – en l'occurrence la CEDH – définisse, par la force des choses, les motifs licites d'ingérence de manière très générale ne signifie pas que le législateur national ne devrait pas tenter de parvenir à un niveau supérieur de précision et de sécurité juridique (voir, *supra*, la section V.C).

89. Deuxièmement, rien ne permet de faire la distinction entre les cas où l'ingérence dans le droit à la vie privée résulte d'une interception de communication transmise par radio ou par câble[54].

90. Troisièmement, en ce qui concerne la question de savoir quels sont les droits énoncés dans la Convention pouvant être affectés par la surveillance stratégique, les principales dispositions pertinentes sont les articles 8 et 13. Toutefois, dans *Weber et Saravia*, la Cour a considéré que la première requérante, une journaliste, aurait également pu prétendre que ses droits en vertu de l'article 10 ont été affectés[55]. D'autres instances ont confirmé que les libertés d'expression et d'information sont également en jeu dans ce contexte. Les juges de Strasbourg ont à l'occasion mentionné l'effet dissuasif qu'une sanction ou une ordonnance de divulgation de l'identité d'une source peut avoir sur un journaliste[56]. En outre, comme noté *supra*, ils ont déjà souligné que, dans le contexte de la sécurité, il est possible de se prévaloir du droit de rechercher des informations[57]. La CJUE a, elle aussi, relevé l'effet dissuasif que la rétention générale de métadonnées peut avoir sur la liberté d'expression et d'information[58], de même que les rapporteurs spéciaux des Nations Unies et de la Commission interaméricaine des droits de l'homme[59].

91. Quatrièmement, la Cour a expliqué que la surveillance stratégique implique de multiples ingérences dans la vie privée. La première se produit en cas d'octroi d'une autorisation d'intercepter des télécommunications, c'est-à-dire lorsque la loi prévoit que les entreprises de télécommunication doivent permettre au service de ROEM d'accéder selon certaines modalités à toutes les communications ou seulement à certaines catégories d'entre elles, ou bien que ledit service est habilité à acquérir toutes les communications ou seulement certaines catégories d'entre elles. Comme expliqué *supra* dans la section IV, dans le cadre de la surveillance stratégique du contenu, le matériel réellement examiné est obtenu en effectuant des recherches sur les renseignements en vrac acquis au moyen d'algorithmes informatiques (sélecteurs). Par conséquent, si l'on suit l'approche de la Cour jusqu'au bout, il

[54] Cela résulte du fait que la Cour s'abstient de mentionner cette distinction aussi bien dans ses décisions *Liberty et autres c. Royaume-Uni* que *Weber et Saravia c. Allemagne*.

[55] *Weber et Saravia c. Allemagne*, paragraphe 145 « […] les télécommunications passées par l'intéressée à des fins journalistiques risquent d'être surveillées et ses sources journalistiques d'être révélées ou dissuadées d'appeler et de fournir des informations par téléphone […] la transmission de données à d'autres autorités, leur destruction et l'absence de notification à la première requérante des mesures de surveillance sont de nature à compromettre la confidentialité et la protection des renseignements donnés à l'intéressée par ses sources ». D'aucuns pourraient faire valoir, en invoquant l'article 16 de la CEDH, que les journalistes étrangers devraient jouir exactement des mêmes droits consacrés par l'article 10 que les nationaux. Toutefois, la Cour a précisé que cet article doit être interprété de manière restrictive (*Piermont c. France* [27 avril 1995], A/314).

[56] Voir, par exemple, *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, Requête n° 39315/06, 22 novembre 2012.

[57] *Youth Initiative for Human Rights c. Serbie*, voir *supra*.

[58] CJUE, arrêt rendu par la Grande Chambre le 8 avril 2014 dans l'affaire « Digital Rights Ireland Ltd », paragraphe 28.

[59] Déclaration conjointe du rapporteur spécial des Nations Unies sur la protection et la promotion du droit à la liberté d'opinion et d'expression et du rapporteur spécial pour la liberté d'expression de la Commission interaméricaine des droits de l'homme, www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

appartiendra à une autorité légale de déterminer les sélecteurs applicables au contenu des données et, en ce qui concerne les métadonnées, de donner des instructions concernant la construction du graphe social et les modalités des autres analyses.

92. La deuxième ingérence tient à ce que les données en vrac, après avoir été traitées et analysées, sont transmises et utilisées par des autorités autres que le service de ROEM. Troisièmement et dernièrement, la Cour considère qu'il y a ingérence dans la vie privée dès lors que les règles prévoient la destruction des données obtenues, mais pas la notification aux personnes concernées des mesures de surveillance adoptées[60]. En d'autres termes, une autorité légale spécifique – accessible et agissant en conformité à la jurisprudence de Strasbourg relative à la qualité de la loi – doit pouvoir répondre de chacune de ces ingérences.

93. Cinquièmement, la Cour a souligné la nécessité d'une législation principale régissant les principaux éléments de la surveillance secrète. La jurisprudence, même lorsqu'elle formule des règles détaillées et émane de la Cour suprême ou constitutionnelle, n'est pas plus suffisante en elle-même – pour réglementer cette activité[61] – qu'une législation secondaire. Le but de la définition précise des pouvoirs est de réduire la portée d'une éventuelle utilisation abusive ou excessive. Lorsqu'un pouvoir est défini de manière vague par une loi et que le contrôle se limite à vérifier que le service n'a pas débordé son mandat légal, ledit contrôle ne présente que peu d'intérêt[62]. En outre, toutes choses étant égales par ailleurs, plus le pouvoir en question affecte la vie privée, plus son utilisation abusive ou excessive risque de provoquer des dommages importants. La précision favorise la conscience à tout moment, par le personnel chargé de mener l'enquête et de délivrer les autorisations, de ses responsabilités : une attitude renforcée par la perspective d'une éventuelle condamnation pénale pour abus de pouvoir en cas de manquement. Pourtant, l'essentiel de la question dans ce domaine tient à savoir quelles sont les parties du système qui pourraient faire l'objet d'une réglementation interne, c'est-à-dire secrète (voir aussi, *infra*, le paragraphe 107). Pour répondre à cette question, il convient de dépasser la lettre de la loi pertinente pour s'interroger sur ses valeurs sous-jacentes normalement au nombre de trois : la prévisibilité/stabilité, la légitimité démocratique et la compétence institutionnelle. Une réglementation énoncée dans une loi matérielle est plus stable et plus transparente qu'un ensemble de normes fixé par une législation secondaire. En outre, il appartient aux représentants du peuple de mettre en balance des intérêts concurrents dans un domaine aussi important. La troisième valeur tient au temps et aux compétences dont dispose le parlement pour concevoir des règles générales appropriées ainsi qu'au caractère complet du débat (lequel prend notamment en considération tous les facteurs pertinents) qui précède ou devrait précéder l'adoption de tout projet de loi. En tout cas, la Cour a rejeté, dans l'affaire *Liberty et autres*, les arguments du Gouvernement britannique faisant valoir qu'il faudrait abaisser les critères d'accessibilité[63]. La Cour a déclaré dans son arrêt ne voir « aucune raison de soumettre les règles gouvernant l'interception de communications

[60] *Op. cit.*, paragraphe 79. Dans l'affaire *Liberty et autres c. Royaume-Uni*, la Cour s'est contentée de déclarer que « l'existence de ces pouvoirs – en particulier ceux autorisant l'analyse, l'utilisation et la conservation des données interceptées – s'analyse en une ingérence dans les droits des intéressées au titre de l'article 8 puisque celles-ci étaient susceptibles de se voir appliquer les pouvoirs en question » (paragraphe 57).

[61] Voir *Heglas c. République tchèque*, Requête n° 5935/02, 1er mars 2007, paragraphe 74.

[62] Par exemple, d'aucuns critiquent l'étroitesse du champ de l'examen par l'IPT (voir, *infra*, le paragraphe 96). Voir notamment : « Justice : Freedom from suspicion : surveillance reform for a digital age » (2011), p. 133 à 153; Leigh, I., « A view from across the channel: intelligence oversight in the UK », *in* W. van Laethem, J. Vanderborght, (éd.), *Regards sur le contrôle*, Intersentia, Anvers, 2013.

[63] L'importance accordée en l'instance par la Cour aux exigences en matière d'accessibilité tient probablement au pouvoir d'appréciation très large – en fait « pratiquement illimité » (paragraphe 64) – conféré par la législation britannique à l'organe d'autorisation.

individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents ».

94. La Cour a ensuite procédé à l'élaboration de la liste des questions qui devraient être couvertes par une loi, en se référant à sa décision rendue antérieurement dans l'affaire *Weber et Saravia* :

> « [la loi G10] autorisait en particulier le service fédéral des renseignements à exécuter des mesures de surveillance uniquement à l'aide de mots-clés utiles et adaptés aux investigations portant sur les dangers décrits dans le mandat de surveillance et énumérés dans celui-ci […] Les autorités qui conservaient les données devaient vérifier tous les six mois si celles-ci demeuraient nécessaires à la poursuite des buts pour lesquels elles avaient été recueillies ou leur avaient été transmises. Si tel n'était pas le cas, ces données devaient être détruites et effacées des fichiers ou, tout au moins, leur accès devait être interdit ; la destruction devait être consignée dans un procès-verbal et, dans les cas envisagés par l'article 3, paragraphe 6, et l'article 7, paragraphe 4, contrôlée par un agent possédant les qualifications requises pour accéder à la magistrature. La loi G10 renfermait d'autres dispositions précises régissant la transmission, la conservation et l'utilisation de renseignements obtenus au moyen de l'interception de communications à destination ou en provenance de l'étranger […] »[64].

95. Sixièmement, même si la Cour ne semble pas s'être directement penchée sur la question, il résulte logiquement de ces conclusions relatives à l'accessibilité des données qu'une autorité légale spécifique et distincte devrait être chargée de contrôler les autres méthodes éventuellement utilisées par les services de ROEM pour obtenir des données. L'une de ces méthodes consiste à obtenir des données brutes en vrac auprès d'homologues de pays amis. Telle était justement la principale question analysée par le tribunal britannique chargé de juger les abus de pouvoir en matière d'enquête (IPT) dans son arrêt rendu dans une affaire où un certain nombre d'ONG avait introduit une requête contre le service de ROEM du Royaume-Uni (le CGHQ). Ce dernier et le Gouvernement britannique avaient assuré l'IPT que le matériel ainsi transmis ne pouvait faire l'objet de recherches qu'après obtention d'une autorisation délivrée selon des règles identiques à celles régissant l'octroi d'une autorisation de recherche dans les données en vrac collectées par le GCHQ lui-même. Toutefois, aucune autorisation préalable de la sorte n'avait été obtenue en l'espèce avant le transfert. C'est pourquoi le tribunal a conclu que, au cours de la période ayant précédé les divulgations, les recherches menées par le GCHQ dans le matériel transféré n'étaient pas « prévues par la loi ».

96. Comme indiqué *supra* dans la section IV, un service de ROEM, avec (ou parfois sans) l'accord des FAI, peut être en mesure d'accéder à des données conservées, notamment celles stockées dans le « cloud ». Il convient à ce propos de faire remarquer que, même lorsqu'un FAI donne son accord, aucun pays européen tenu aux obligations découlant des principes de protection des données ne saurait valablement prétendre qu'un tel accès ne s'analyse pas en une ingérence dans la vie privée et/ou dans la liberté de correspondance[65]. En ce qui concerne de telles données à caractère personnel, l'ingérence se produit même lorsque leur « propriétaire » ou contrôleur légal donne son consentement. Par conséquent, il faut également qu'une autorité légale puisse contrôler ce pouvoir d'accès sans consentement. Il en va de même en ce qui concerne le pouvoir encore plus controversé de

[64] *Op. cit.*, paragraphe 68.

[65] Voir, par exemple, l'arrêt 2 BvR 902/06 de la Cour constitutionnelle fédérale allemande dans lequel cette juridiction a considéré que les courriels conservés sur un serveur sont protégés en vertu du droit constitutionnel à la liberté de communication.

s'introduire illégalement à distance dans des ordinateurs pour y implanter un logiciel malveillant. Cette mesure équivaut à une perquisition suivie d'une saisie, à la différence qu'elle est secrète et produit ses effets pendant toute la période de fonctionnement du logiciel. Sur la base de la jurisprudence de la Cour, l'autorisation de telles pratiques, à supposer qu'elle soit accordée, ne serait valable que pour une liste très courte d'infractions et assortie de conditions très claires en matière d'autorité légale, d'autorisation juridictionnelle[66], de minimisation et de destruction, le tout dans le cadre d'un régime strict de contrôle compte tenu de sa nature secrète[67].

B. Adaptation des normes de la Cour européenne des droits de l'homme à la surveillance stratégique

97. Pour en venir à la question de l'adaptation des garanties élaborées par la Cour en matière de surveillance ordinaire à la surveillance stratégique[68], la première de ces garanties vise la nature des infractions pouvant faire l'objet d'une ordonnance d'interception. Elle s'applique principalement aux États qui prévoient la possibilité de recourir au ROEM aux fins d'enquête sur des infractions relevant de la sécurité ou autres crimes graves comme le blanchiment qualifié de capitaux. Ces juridictions sont tenues d'énumérer les infractions pertinentes et de prévoir la destruction des données pouvant être incidemment collectées sur d'autres infractions. L'exception à cette règle – en vue de permettre le transfert de données aux autorités répressives – doit être définie avec précision et soumise à un contrôle, car on risquerait autrement de voir l'exception devenir la règle et la garantie perdre sa valeur[69] ; ladite garantie est pertinente en ce qui concerne à la fois la construction d'un graphe social sur la base de métadonnées et les recherches visant les données de contenu.

---

[66] Voir, par exemple, la législation belge qui confie à une commission de contrôle quasi judiciaire la tâche de donner un avis contraignant préalable au service de sécurité envisageant de recourir à cette mesure et à d'autres « méthodes exceptionnelles » (loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité de 1998, article 18, paragraphes 2 et 3, modifiée par la loi du 4 février 2010).

[67] Voir, par exemple, *Wieser et Bicos Beteiligungen Gmbh c. Autriche*, Requête n° 74336/01, 16 octobre 2007 (concernant le caractère disproportionné de la saisie physique d'ordinateurs dans un bureau d'avocats). Voir également l'arrêt 1 BvR 595/07 rendu par la Cour constitutionnelle fédérale allemande qui a estimé que, compte tenu de la gravité de l'ingérence, l'infiltration secrète d'un système de technologie de l'information en vue de sa surveillance et de l'accès à ses supports de stockage n'est constitutionnellement admissible qu'en présence d'indications factuelles d'un danger concret pesant sur un intérêt juridique revêtant une importance prioritaire. Parmi ces « intérêts juridiques significatifs » figurent la vie humaine et la liberté individuelle, ainsi que la protection contre les menaces publiques pouvant affecter l'existence continue de l'État. Les juges de Karlsruhe ont également conclu à la nécessité d'imposer des garde-fous, une autorisation judiciaire, la minimisation et la destruction des données.

[68] On peut mentionner dans ce contexte une garantie n'étant pas pertinente sous l'angle de la surveillance ciblée, à savoir une restriction quantitative. Par exemple, l'article 10(4) de la loi allemande G10 prévoit que l'ordonnance d'acquisition d'un contenu en vrac « doit préciser la proportion de la capacité de transmission disponible sur ces trajets de transmission qui pourront faire l'objet d'un contrôle. Dans le cadre [d'une surveillance stratégique], cette proportion ne peut pas dépasser 20 % ». Les proportions respectées en pratique sont considérablement inférieures. Toutefois, même une proportion de 8 % du trafic représente un volume considérable. La législation suédoise ne fixe pas une proportion maximale du trafic, mais impose l'identification des porteurs de signaux et interdit la collecte de données en vrac si l'objectif poursuivi peut être atteint d'une manière moins restrictive, sauf si la valeur de l'information que l'on compte tirer de l'acquisition des données est nettement supérieure au dommage potentiel associé à l'ingérence dans la vie privée (article 5). Cette condition est appliquée par l'organe d'autorisation juridictionnel et vérifiée par l'organe extérieur de contrôle (voir, *infra*, les paragraphes 120-122), dans la mesure où de telles limites doivent manifestement faire l'objet d'un contrôle externe pour avoir un sens.

[69] Par exemple, dans le cadre de son évaluation de la constitutionnalité des modifications apportées à la loi allemande, la BVerfG a ajouté un garde-fou : plus l'infraction est mineure, plus les indications de sa commission par une personne donnée devront être manifestes pour que le transfert d'informations soit autorisé, BVerfG, 1 BvR 2226/94, 2420/95 et 2437/95, 14 juillet 1999. L'article 7 de la loi G10 dresse la liste exhaustive des autorités auxquelles le service de ROEM peut transférer des renseignements et des motifs d'un tel transfert. Son paragraphe 7.*a* énonce les conditions pesant sur le transfert de renseignements d'origine électromagnétique à des services étrangers.

98. Une autre garantie tient à la définition des catégories de personnes pouvant voir leurs communications interceptées. En d'autres termes, il convient de préciser l'étroitesse du lien des personnes en question avec l'infraction (ou avec la conduite portant atteinte à la sécurité nationale). Lesdites personnes incluent de toute évidence les individus soupçonnés d'une des infractions énumérées, mais la loi peut également prévoir que les personnes en contact **avec les intéressés sont susceptibles, elles aussi, dans certaines circonstances, de faire** l'objet d'une interception de leurs télécommunications. En ce qui concerne la construction d'un graphe social sur la base de métadonnées, ce procédé ne peut concerner normalement que les personnes soupçonnées d'avoir réellement pris part à des infractions particulièrement graves comme le terrorisme. Lorsqu'une telle personne (A) est en contact avec d'autres (B, C, D), l'inclusion de ces dernières dans le graphe social n'est possible que s'il existe des raisons distinctes de soupçonner les intéressés de participation à des activités terroristes[70]. En revanche, à supposer que le pouvoir de construire un graphe social soit défini en termes d'un simple lien pertinent avec l'enquête pour terrorisme, et même si une norme en matière de preuve (par exemple « un soupçon plausible ») s'applique, une telle approche risque d'agrandir sensiblement le filet de surveillance. Par exemple, à supposer que le suspect initial ait 100 contacts ayant eux-mêmes chacun 100 contacts, on peut facilement concevoir que le filet risque de grandir de manière exponentielle et d'attraper dans ses mailles une foule de gens n'ayant pas le moindre lien avec le terrorisme. On peut difficilement comprendre comment une approche aussi large de la construction du graphe social pourrait être considérée comme proportionnelle (ou s'analyser en une utilisation judicieuse des ressources du service de ROEM)[71].

99. L'une des méthodes utilisées pour essayer de limiter une approche trop large du graphe social consiste à restreindre strictement le pouvoir d'interroger les métadonnées collectées en vrac[72]. Une autre consiste à créer un défenseur de la vie privée, c'est-à-dire un mécanisme institutionnel en mesure de protéger les personnes n'ayant rien à faire avec l'infraction objet de l'enquête. Le défenseur peut soulever des arguments au nom des intéressés et tenter de limiter autant que faire se peut les paramètres de recherche au moment du ciblage[73].

100. En ce qui concerne les recherches portant sur des données de contenu, les problèmes d'ingérence dans la vie privée sont souvent soulevés lorsqu'on envisage d'utiliser un sélecteur associé à une personne physique (par exemple son nom, son surnom, son adresse électronique ou physique, etc.). Le renforcement des exigences en matière de justification et des garanties de procédure ne devrait s'appliquer qu'à des situations de ce type, sous la forme notamment de la participation d'un défenseur de la vie privée au processus. Des garanties sont également nécessaires concernant les décisions subséquentes de transférer des renseignements relatifs à des individus obtenus dans le

[70] En ce qui concerne la pratique des États-Unis, voir *infra* le paragraphe 117.

[71] Le PCLOB a conclu que le programme de l'article 215 de la NSA ne répond pas aux critères d'efficacité et a donc recommandé d'y mettre fin. PCLOB, « Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court », 23 janvier 2014.

[72] Il convient de noter à ce propos que, en vertu de la Directive (annulée) de l'UE sur la conservation des données, les métadonnées pouvaient être conservées pendant deux ans au plus et faire l'objet de recherches dans le cadre d'une enquête visant « une grave infraction ». Le caractère vague de ce terme avait contribué à l'abrogation de cet instrument.

[73] Selon certaines preuves empiriques, la présence de défenseurs de la vie privée dans le système de contrôle des autorités répressives et des organes de sécurité intérieure peut contribuer, dans une certaine mesure, à une définition aussi étroite que possible des paramètres d'enquête. Voir l'enquête officielle menée en Suède sur la surveillance secrète, SOU 2012:44. Les défenseurs de la vie privée (proposés par l'association du barreau et nommés par le gouvernement) représentent les intérêts des personnes et organisations ciblées devant le tribunal suédois du renseignement militaire (voir, *infra*, le paragraphe 132).

cadre d'une surveillance stratégique au service de sécurité intérieure, aux autorités répressives ou à des services étrangers[74].

101. La Cour estimait que seules deux catégories de personnes méritent une protection spéciale : d'une part les avocats et autres personnes habilitées à entretenir « des communications privilégiées » comme les prêtres et, d'autre part, les journalistes. L'un des garde-fous applicables à la surveillance ordinaire consiste à imposer l'effacement des « communications privilégiées ». En d'autres termes, les personnes concernées ne devraient pas normalement être ciblées dans le cadre de la construction d'un graphe social sur la base de métadonnées ou de l'utilisation de sélecteurs. De plus, à supposer que leurs communications aient été indirectement attrapées dans le filet, elles devraient être détruites sous le contrôle d'un « gardien » interne juridiquement qualifié ou d'un organe de supervision externe. Selon la jurisprudence de la Cour – élaborée notamment dans *Klass c. RFA*, *Kopp c. Suisse* et, plus récemment, dans l'arrêt *Erdem c. Allemagne* qui portait sur une affaire d'interception[75], la Convention n'oblige pas les États à s'abstenir totalement de toute surveillance des « communications privilégiées ». Mais – sauf preuve de la participation de l'avocat, du prêtre, etc., en cause dans l'infraction ou de la conduite dommageable pour la sécurité nationale – l'interception au moyen de la collecte de signaux d'origine électromagnétique devrait être illégale[76].

102. Les journalistes constituent un autre groupe méritant une protection spéciale. Il convient de tenir compte, en ce qui les concerne, de leur fonction de donneur d'alerte. Le fait de construire le graphe social d'un journaliste pourrait aboutir à l'identification de ses sources. Pour un fonctionnaire, même le risque potentiel d'une telle identification pourrait être totalement dissuasif et l'empêcher de transmettre des informations à un journaliste. Cela dit, on ne saurait édicter une interdiction absolue de construction du graphe social d'un journaliste en présence de fortes raisons de recourir à une telle pratique (le plus souvent parce que l'intéressé aurait contribué à la fuite d'informations ultrasecrètes). Il convient de mentionner en outre la difficulté associée à la définition de la profession. À la différence des avocats et des prêtres, les journalistes ne sont pas toujours facilement différenciables ; les ONG vouées à la formation de l'opinion publique ou même les bloggeurs pourraient revendiquer à juste titre des protections équivalentes.

103. Une solution consiste à leur accorder un niveau de protection analogue à celui des avocats et des autres communicants privilégiés. Une autre passe par la fixation d'un seuil élevé ou très élevé devant être atteint pour que l'opération prévoyant la collecte de ROEM sur un journaliste soit autorisée, combinée à des garanties de procédure et à un étroit contrôle par un organe extérieur. La collecte indirecte d'informations sur des journalistes est, relativement parlant, plus probable (compte tenu des méthodes de travail des intéressés), de sorte qu'il conviendrait en l'occurrence d'imposer des obligations de destruction et de veiller correctement à leur respect.

104. Imposer une limite de temps ne constitue pas un garde-fou aussi efficace en matière de surveillance stratégique qu'en matière de surveillance ordinaire. Cette dernière est en effet onéreuse puisqu'elle implique l'écoute par des analystes en chair et en os des communications interceptées et, parfois aussi, leur traduction. Du point de vue de l'efficacité, la surveillance exercée par les autorités répressives ou un service de sécurité intérieure ne

[74] Ainsi, la BVerfG a estimé que les arrangements en matière de conservation et d'utilisation des informations par le service de renseignement [article 3(4)] et le transfert d'informations au gouvernement [article 3(3)] n'étaient pas définis avec suffisamment de précision dans la loi initiale.

[75] Requête n° 38321/97, 5 juillet 2001.

[76] À titre d'exemple, la loi G10 allemande (article 3.*b*) et la loi suédoise sur le renseignement d'origine électromagnétique (article 7) prévoient toutes deux la destruction des communications privilégiées.

peut pas normalement non plus durer très longtemps. Il n'en va pas forcément de même en matière de surveillance stratégique. Les périodes de surveillance ont tendance à être longues et continuellement renouvelées. Les périodes de conservation sont fréquemment étendues aussi car des données perçues initialement comme sans intérêt peuvent s'avérer, au fur et à mesure de l'arrivée de nouvelles informations, comme pertinentes[77]. Il est cependant possible, comme c'est le cas dans la législation allemande telle qu'elle est décrite ci-dessus, d'imposer l'obligation de procéder périodiquement à un contrôle interne du besoin (persistant) de conserver les données. Néanmoins, pour qu'un tel système s'avère efficace, il est indispensable que le respect de cette obligation soit vérifié par un organe de contrôle externe.

105. Il semble que les deux garanties les plus importantes soient le processus d'autorisation (de la collecte *et* de l'accès aux données collectées) et le processus de suivi (contrôle). Il ressort nettement de la jurisprudence de la Cour que ce dernier processus doit être confié à un organe indépendant et extérieur. La question qu'il convient de se poser dans ce contexte est de savoir si le processus d'autorisation devrait, lui aussi, être indépendant.

106. Comme indiqué *supra*, dans la section V.D, dans certains États comme le Royaume-Uni ou les Pays-Bas l'organe chargé de délivrer l'autorisation est le ministre compétent, c'est-à-dire une personne ne pouvant en aucun cas être considérée comme indépendante par rapport à l'exécutif. Dans *Popescu c. Roumanie*[78], la Cour a considéré que l'autorité roumaine ayant ordonné de procéder à la surveillance (en l'occurrence un procureur) n'était pas indépendante par rapport à l'exécutif. Elle a souligné l'importance de cette indépendance et la nécessité de prévoir un contrôle juridictionnel ou indépendant de l'activité de l'autorité délivrant les autorisations. De même, dans les affaires *Iordachi* et *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, la Cour a souligné qu'il faudrait prévoir des contrôles indépendants à la fois au stade de l'autorisation et à celui du suivi. Les juges de Strasbourg ont une préférence pour le système d'autorisation juridictionnel même si, dans l'affaire *Kennedy c. Royaume-Uni*[79], ils ont accepté le régime britannique d'autorisation ministérielle. Il se pourrait que la Cour exige l'application de normes plus élevées en présence de preuves de l'inobservation de la loi en pratique. Quoi qu'il en soit, si l'on opte pour une approche holistique consistant à évaluer le système dans son ensemble, il semble clair que l'absence dans un système de contrôles indépendants au stade de l'autorisation devrait être compensée par des garanties extrêmement solides au stade du suivi/contrôle, garanties pouvant notamment se traduire par l'octroi à l'organe de contrôle du pouvoir de rendre des décisions contraignantes[80]. De plus, bien entendu, chaque État peut se doter de normes constitutionnelles plus strictes exigeant l'indépendance à la fois du processus d'autorisation et de celui de contrôle.

---

[77]. C'est la raison principale pour laquelle le rapport du Conseil national de la recherche des États-Unis a considéré qu'il pourrait s'avérer problématique d'imposer des limites supplémentaires à la collecte. En revanche, le renforcement des limites lors de l'accès subséquent aux données en vrac collectées pourrait être un moyen de réduire les risques d'abus (*op. cit.*, p. 51).

[78] Requête No 71525/01, 26 avril 2007

[79] Requête No 26839/05, 18 mai 2010

[80]. Voir notamment les pouvoirs octroyés à la commission G10 en Allemagne (voir, *infra*, le paragraphe 112) ou à la SIUN suédoise (Inspection du renseignement militaire – Statens inspektion för försvarsunderrättelseverksamheten) (voir, *infra*, le paragraphe 121).

VII. Contrôle interne et contrôle gouvernemental, éléments de systèmes de contrôle globaux

107. Comme indiqué dans le rapport de 2007, les contrôles internes constituent la principale garantie en présence d'un service respectueux du droit et qui n'abuse pas de son pouvoir. À cet égard, les procédures de recrutement et de formation revêtent une importance clé[81]. Les règles internes précisent de manière plus détaillée les obligations énoncées dans la loi et sont donc particulièrement importantes dans le domaine du ROEM, même si elles doivent rester secrètes par la force des choses. Il est donc indispensable d'exiger du service de tenir compte de la protection de la vie privée et des autres droits de l'homme lorsqu'il promulgue des règles internes[82]. Pour les raisons avancées dans la section IV, il peut s'avérer particulièrement tentant de se reposer principalement sur les contrôles internes en matière de surveillance stratégique. Les systèmes néerlandais et britannique d'autorisation par le ministre compétent – si l'on tient compte de l'emploi du temps de l'intéressé et de ses nombreuses autres responsabilités – aboutissent en fait à rendre celui-ci totalement dépendant des hauts fonctionnaires qui lui servent de collaborateurs. Pourtant, pour les raisons énoncées dans le rapport de 2007, les contrôles internes sont insuffisants. Comme nous l'avons déjà indiqué, la conséquence logique de l'absence d'un mécanisme d'autorisation préalable indépendant est le renforcement des mécanismes de contrôle *post hoc*. Le Conseil de la commission présidentielle compétente des États-Unis a également constaté l'inanité d'un système reposant principalement sur des contrôles internes et souligné la nécessité d'un renforcement considérable de la supervision exercée sur la NSA[83].

VIII. Contrôle par le parlement

108. La supervision par le parlement de la surveillance stratégique est problématique à plusieurs titres. Premièrement, le caractère extrêmement technique du renseignement d'origine électromagnétique explique que les parlementaires ont beaucoup de mal à exercer leur supervision sans l'aide de spécialistes. Deuxièmement, le problème général du peu de temps que les parlementaires peuvent accorder à cette supervision en raison de leurs nombreuses autres responsabilités revêt une acuité particulière en ce qui concerne la surveillance stratégique. Dès lors qu'une personne désire contrôler le processus dynamique d'affinage des sélecteurs (et non pas exercer un simple contrôle *post hoc*), elle a besoin d'un organe permanent. Troisièmement, la coopération étroite en réseau entre différents services de ROEM explique la réticence accrue à l'idée d'un contrôle exercé par le parlement : une attitude qui risque donc d'affecter non seulement les services d'un pays donné, mais également ceux des pays alliés. Comme indiqué précédemment, dans certains États, la doctrine du privilège parlementaire signifie qu'il est impossible de soumettre les membres des commissions du parlement à une procédure de contrôle de sécurité, ce qui ne fait qu'accroître la peur des fuites. L'autre facteur crucial tient à ce que la supervision

[81] L'organe de contrôle externe suédois, la SIUN (voir, *infra*, le paragraphe 121) est expressément tenu, en vertu de la loi, de suivre les questions de recrutement et de formation. Plusieurs des recommandations du rapport du PCLOB sur l'article 702 portent sur la sensibilisation accrue, dans le cadre de la formation, aux questions associées à la vie privée.

[82] Sur ce point, il convient de noter que l'institutionnalisation de la protection des droits de l'homme passe à la fois par la définition de règles internes et, en raison de l'importance des systèmes automatisés de minimisation, par la « traduction » de ces mêmes règles dans les logiciels pertinents.

[83] Selon ce conseil : « Les Américains ne doivent pas commettre l'erreur de faire confiance aux agents publics responsables », in *Liberty and Security in a Changing World, op. cit.*, p. 114. Le contrôle externe peut contribuer à renforcer la culture interne du service de nombreuses façons. En Suède, par exemple, le service de ROEM dispose d'un « conseil pour l'intégrité » composé de trois juges chargés de donner leur avis en cas d'élaboration de règles internes.

stratégique implique une ingérence dans les droits individuels. Le contrôle des mesures de ce type relève traditionnellement du judiciaire. Le principe constitutionnel de séparation des pouvoirs s'oppose donc, dans une certaine mesure, à ce qu'un organe parlementaire assume ainsi un rôle quasi judiciaire.

109. Il paraît opportun à ce stade de revenir un peu plus en détail sur ce dernier point : comme il a été démontré dans les sections précédentes, il est nécessaire – à plusieurs étapes du processus – de mettre en balance divers droits individuels, dont la protection de la vie privée, d'une part, et d'autres intérêts, d'autre part, mais deux stades revêtent une importance particulièrement cruciale de ce point de vue : celui de la décision de recourir à certains sélecteurs et celui de la décision d'un analyste en chair et en os de conserver ou pas l'information en question. Le premier type de décisions s'apparente, du moins sous certains aspects, à une décision d'autorisation d'une surveillance ciblée et, à ce titre, peut relever d'un organe juridictionnel. Dans la mesure où chaque décision implique la prise en considération d'éléments politiques, il est souhaitable que les décideurs aient, outre des compétences juridiques, une bonne connaissance à la fois des techniques de renseignement et de l'état des relations extérieures de leur pays. Il peut s'avérer difficile, même pour un grand pays, de trouver des personnes alliant ces trois types de compétences, de sorte que la solution peut passer par la création d'un organe hybride réunissant des juges et d'autres spécialistes.

110. Le second type de décisions concerne la « protection des données », c'est-à-dire une activité qui peut être contrôlée a posteriori par un organe administratif spécialisé, indépendant et doté de pouvoirs appropriés[84]. Aucun de ces types de décisions ne revêt un caractère véritablement « politique ». En revanche, la décision initiale de considérer une personne ou une chose suffisamment importante sous l'angle de la sécurité nationale pour mériter que l'on collecte des renseignements à son sujet revêt, elle, un caractère plus « politique ». Chaque décision de ce type gagnerait à être prise à l'issue d'une discussion (à huis clos) par un organe politique au sein duquel divers courants d'opinion sont représentés. La définition des règles générales déterminant qui peut collecter ou échanger des ROEM[85] avec des homologues[86] et selon quelles modalités constitue, elle aussi, une question revêtant un caractère politique. Le troisième type de décisions concerne l'évaluation générale de l'efficacité globale des mesures relatives à la collecte et au traitement des renseignements d'origine électromagnétique. Un quatrième rôle d'un organe politique est d'engager un dialogue continu avec tous les organes de supervision compétents.

111. Deux modèles parlementaires méritent d'être mentionnés dans ce contexte. Dans le domaine du contrôle, il convient d'avoir à l'esprit que, même si l'organe compétent doit disposer de pouvoirs suffisants sur le papier, c'est en réalité la manière dont il exerce lesdits pouvoirs en pratique qui est importante. Aux États-Unis, les commissions du renseignement du Sénat et de la Chambre des représentants ont droit à intervalles réguliers à des séances d'information au cours desquelles des membres des services de renseignement abordent différents sujets, dont le fonctionnement de la surveillance stratégique exercée par la NSA. Pourtant, plusieurs personnes – à savoir des membres d'autres commissions parlementaires

[84] Voir, *infra*, les paragraphes 124 et 132. En ce qui concerne l'indépendance des organes de protection des données, voir la Directive 95/46 de l'UE et le Protocole additionnel (2001) 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 (STCE n° 181). Il est également possible pour un organe administratif spécialisé d'exercer des fonctions de recours (voir, *infra*, les paragraphes 137 et 138).

[85] Voir, par exemple, les auditions organisées par l'ISC (Intelligence and Security Committee) britannique afin de permettre aux organisations non gouvernementales d'exprimer leurs opinions sur la question : http://isc.independent.gov.uk/public-evidence.

[86] En tout cas, ces arrangements de portée générale devraient faire l'objet d'une certaine forme d'autorisation par un organe extérieur. Voir, par exemple, Parlement européen, *op. cit.*, p. 218.

ou des universitaires – ont exprimé des critiques concernant le contrôle exercé par ces commissions en matière de surveillance stratégique[87]. Il est certain que, en raison de la taille des services de renseignement des États-Unis ainsi que de la variété et de la complexité des questions devant faire l'objet d'un suivi, ces commissions parlementaires se sentent obligées de focaliser leur attention sur tel ou tel problème particulier, comme n'a pas manqué de le faire la commission du Sénat lorsqu'elle s'est attachée à examiner le programme de restitution (*rendition*) de la CIA. En outre, pénétrer le monde mystérieux du renseignement d'origine électromagnétique passe par l'identification des questions pertinentes à formuler, lesquelles devront être posées à plusieurs reprises en faisant preuve d'une obstination particulière. Les membres de la commission compétente du Sénat peuvent se faire assister par des personnes de leur propre équipe (à condition que les intéressés disposent des autorisations de sécurité requises), ce qui n'est pas le cas de leurs homologues de la commission de la Chambre des représentants. Dans certains cas particuliers, en raison de la nature classifiée du matériel discuté, le contrôle exercé par le Congrès se heurte à plusieurs obstacles : fragmentation[88], limitations telles que l'interdiction de faire sortir des informations communiquées pendant des séances d'information ou des notes de certaines zones spécialement délimitées du Capitole, ou interdiction pour les membres du Congrès d'assister en compagnie de leurs conseillers juridiques à des séances d'information[89]. Le Congrès exerce surtout son pouvoir sur les services de renseignement en menaçant ou en promettant d'adopter telle ou telle législation et de veiller à ce que tel ou tel crédit budgétaire soit alloué (bien que ni la commission du renseignement du Sénat ni celle de la Chambre des représentants n'aient le pouvoir d'allouer des crédits). Il est nécessaire de parvenir à un accord politique pour s'acquitter convenablement de ces tâches. D'aucuns peuvent se poser également la question de savoir quel est le prix politique qu'un législateur pourrait payer dans l'opinion publique dès lors qu'il proposerait le renforcement du contrôle sur le ROEM. N'ayant qu'une faible perception des dommages potentiels qui pourraient leur être infligés à titre individuel, les citoyens ne sont pas enclins à exercer des pressions en ce sens en tant qu'électeurs sur leurs représentants (à supposer que quelqu'un subisse un préjudice, il s'agit probablement d'un étranger). En revanche, le grand public craint par-dessus tout que le renforcement du contrôle se traduise par l'incapacité de prévenir la prochaine attaque terroriste d'envergure : un échec dont il tiendrait ses élus responsables. De toute façon, il est révélateur que la principale critique formulée officiellement jusqu'à présent contre le programme de la NSA émane du PCLOB – un organe spécialisé nommé par l'exécutif (même si ses membres sont confirmés par le Sénat) – et non pas de la commission du renseignement du Sénat ou de la Chambre des représentants.

112. Le modèle allemand repose sur un mécanisme à la fois de contrôle et de supervision. En ce qui concerne le contrôle, les télécommunications censées faire l'objet d'une surveillance au titre de risques particuliers sont définies par le ministère fédéral de l'Intérieur de l'Allemagne et doivent être approuvées par le Parlamentarisches Kontrollgremium (PKGr, le Comité du contrôle parlementaire). Cette dernière exerce ainsi un certain degré de contrôle sur l'attribution des tâches et la quantité et les caractéristiques des porteurs des signaux à intercepter. La deuxième étape consiste à approuver les sélecteurs : une décision

[87] Voir notamment A. B. Zegart, « The Domestic Politics of Irrational Intelligence Oversight », *Political Science Quarterly*, 126, 2011, p. 1-27 ; *Wall Street Journal*, 29 juillet 2014 ; *The Washington Post*, 19 août 2013 ; et M. P., Colaresi, *Democracy Declassified : The Secrecy Dilemma in National Security*, Oxford University Press, Oxford, 2014.

[88] Le ministère de la Sécurité intérieure (Department of Homeland Security) rend compte à 92 commissions et sous-commissions du Congrès ; voir Bipartisan Policy Organisation, « Today's Rising Terrorist Threat and the Danger to the United States : Reflections on the Tenth Anniversary of The 9/11 Commission Report », 2014, p. 21.

[89] Voir généralement : www.washingtonpost.com/politics/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html .

prise par le ministère de l'Intérieur sur proposition du BND, mais avec l'aval de l'organe de contrôle spécialisé compétent, à savoir la commission G10. Cette dernière se compose de quatre membres ordinaires et de quatre membres suppléants élus par la PKGr au début de chaque législature et pouvant éventuellement être membres du Bundestag, bien que cette appartenance ne soit pas une obligation. Le président de la commission G10 doit avoir les qualifications requises pour siéger comme magistrat, ce qui explique que cet organe revêt un caractère hybride tout en pouvant revendiquer une légitimité politique puisque ses membres sont élus par la PKGr.

113. En ce qui concerne la surveillance stratégique, la commission G10 vérifie la légalité des sélecteurs (y compris sous l'angle de la proportionnalité). En ce qui concerne le traitement des données, elle contrôle en particulier leur minimisation par le BND. La commission G10 doit être informée chaque fois que se pose la question de savoir si des données relevant du « cœur même » de la vie privée ont été collectées et stockées, et il lui arrive d'avoir à décider s'il convient d'effacer ou de conserver lesdites données. La commission G10 effectue à l'occasion des inspections des banques de données, notamment en vue de vérifier que les données sont effacées conformément aux exigences. Elle doit également être informée des transferts de renseignements aux services de pays amis et en mesure de les superviser[90].

114. En ce qui concerne le contrôle plus général, le gouvernement assume la responsabilité particulière de fournir chaque semestre à la PKGr des statistiques concernant l'utilisation de la loi G10 et le transfert de données à caractère personnel – obtenues dans le cadre de la surveillance stratégique – à des autorités publiques étrangères (par exemple le service de renseignement d'un pays ami) ou à des organismes supranationaux ou intergouvernementaux. La PKGr dispose de ses propres pouvoirs et ressources en matière d'enquête. Par conséquent, pour schématiser, la PKGr s'occupe des questions revêtant un caractère politique tandis que la commission G10 exerce le contrôle quasi judiciaire des sélecteurs, ainsi que le contrôle administratif des banques de données.

IX. Contrôle et autorisation juridictionnels

115. L'étendue du contrôle et de l'autorisation juridictionnels de la surveillance stratégique peut prêter à discussion[91].

116. Les États-Unis disposent d'un système d'autorisation juridictionnelle : le Foreign Intelligence Surveillance Court ou FISC qui est en fait un tribunal spécialisé. Alors que cette instance est chargée d'autoriser les surveillances individuelles aux États-Unis depuis 1978, elle joue un rôle plus modeste en matière de contrôle de la surveillance. En vertu de l'article 215 du FISA (Foreign Intelligence Surveillance Act), le gouvernement est tenu de

[90] Il convient de noter que certains commentateurs allemands ont soulevé des questions concernant le personnel et les compétences techniques de la commission G10, ainsi que le temps qu'elle consacre réellement au processus d'approbation dans le cadre de ses réunions mensuelles. Voir, par exemple, les commentaires de F. Roggan, *in* « G10-Gesetz », Nomos, Baden-Baden, 2012.

[91] Il est possible de mettre en place des garde-fous juridictionnels à d'autres stades que l'autorisation/contrôle, notamment lorsqu'on a recours au ROEM dans le cadre de procédures administratives, civiles ou pénales subséquentes, même si la probabilité d'un tel cas de figure est faible. Aux États-Unis, toute « personne lésée » – un terme qui peut aussi désigner des non-ressortissants – doit se voir notifier avant la divulgation ou l'utilisation d'une quelconque information la concernant obtenue dans le cadre de l'article 702, devant un tribunal fédéral ou étatique. L'intéressé peut ensuite demander la suppression des preuves au motif qu'elles ont été acquises illégalement et/ou en violation de l'autorisation délivrée en vertu de l'article 702 (50 USC, paragraphe 1806(e)). C'est à une Cour fédérale de district qu'il appartient de déterminer si l'acquisition des renseignements dans le cadre de l'article 702 était légale et autorisée et la même juridiction est habilitée à supprimer toute preuve ayant été obtenue ou générée illégalement (50 USC, paragraphe 1806(f) et (g)). Voir le rapport du PCLOB sur l'article 702, p. 100.

demander un mandat à l'un des 15 juges du FISC[92]. Ce dernier doit approuver à la fois « l'ordonnance principale » autorisant le programme dans son ensemble et les « ordonnances secondaires » exigeant des opérateurs téléphoniques qu'ils communiquent des informations à la NSA. Chaque ordonnance doit être renouvelée au bout de 90 jours. La procédure suivie par le FISC pour examiner les demandes peut inclure une audition et les juges sont également habilités à recueillir le témoignage de fonctionnaires ayant une bonne connaissance technique de l'application pertinente. Dès la délivrance d'un mandat, l'entreprise de télécommunication concernée est tenue de communiquer des informations à la NSA sur une base périodique. Les métadonnées de téléphonie émanant des différents fournisseurs sont fusionnées et stockées sur les réseaux de la NSA dans le strict respect des restrictions du FISC relatives aux modalités (y compris sous l'angle des délais) de leur consultation. L'accès aux métadonnées conservées suppose une recherche qui doit commencer par l'entrée d'un numéro de téléphone ou d'un autre identifiant associé à une organisation terroriste étrangère. La recherche ne peut avoir lieu que si un haut responsable de la NSA ou un agent public spécialement autorisé détermine la présence « d'un soupçon plausible » de liens entre l'identifiant et une organisation terroriste étrangère faisant l'objet d'une enquête du FBI. La recherche est censée permettre de retrouver des métadonnées relatives aux numéros de téléphone ayant été en contact direct avec la « cible initiale », ce qu'il est convenu d'appeler « le premier cercle ». Elle peut également s'étendre à d'autres « cercles » associés à des degrés supérieurs de séparation, c'est-à-dire à des numéros indirectement liés à la cible initiale. Au début, ni le FISC ni la NSA ne limitaient le nombre de degrés de séparation utilisé en cas de tentative d'établissement d'un lien entre des numéros de téléphone et la cible initiale. En mars 2009, le gouvernement a introduit des modifications dans le logiciel de manière à limiter le nombre de degrés à trois[93]. En janvier 2014, le Président Obama a réduit encore plus le nombre de degrés de séparation pour le ramener à deux[94]. Après avoir été triées, les informations collectées dans le cadre de ces deux degrés peuvent être communiquées à d'autres services de renseignement. En 2015, il a été décidé et annoncé que chaque détermination de la présence d'un « soupçon plausible » – auparavant du ressort du ministère de la Justice – devrait également être approuvée (sauf en cas d'urgence) par le FISC[95].

117. En ce qui concerne l'acquisition en vrac de données de contenu en vertu de l'article 702, l'*attorney general* et le directeur du renseignement national autorisent chaque année en bloc l'acquisition par ciblage de renseignements à l'étranger, sans préciser au FISC l'identité des non-ressortissants américains concernés. Rien n'impose au gouvernement d'apporter la preuve d'une raison plausible de croire qu'un individu ciblé est un agent d'une puissance étrangère. En revanche, les certifications délivrées dans le cadre de l'article 702 identifient les catégories d'informations qu'il convient de collecter, lesquelles doivent être conformes à la définition légale des informations des services de renseignement extérieur[96]. L'article 702 exige du gouvernement qu'il élabore des procédures de ciblage et

[92] Les juges du FISC sont nommés par le Président et choisis parmi les magistrats fédéraux. Leur mandat dure sept ans.

[93] *Memorandum of the United States in Response to the Court's Order Dated January 28, 2009 at 20, In re Prod. of Tangible Things From [REDACTED]*], n° BR 08-13 (FISA Ct. Feb. 17, 2009).

[94] Transcription du discours prononcé par le Président Obama le 17 janvier sur la réforme de la NSA, *The Washington Post*, 17 janvier 2014, www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html (« À compter d'aujourd'hui, nous ne rechercherons plus que les conversations téléphoniques n'étant pas distantes de plus de deux degrés de séparation d'un numéro associé à une organisation terroriste, alors que jusqu'à présent nous allions jusqu'à trois. »).

[95] Pour plus de détails, voir http://icontherecord.tumblr.com/ppd-28/2015/overview.

[96] La définition de l'objet de l'information relevant du renseignement extérieur se limite à : la protection contre les attaques potentielles ou réelles ; la lutte contre le terrorisme international et la prolifération des armes de destruction massive ; les activités de contre-espionnage et la collecte d'informations relatives à une puissance

de minimisation répondant à certains critères. Dans le cadre de l'examen et de l'approbation par le FISC des certifications annuelles délivrées par le gouvernement, ce tribunal doit valider lesdites procédures et déterminer qu'elles répondent aux normes requises. La description des procédures de ciblage et de minimisation doit être communiquée aux commissions du renseignement et des affaires judiciaires du Sénat et de la Chambre des représentants[97].

118. Par conséquent, le FISC définit et valide chaque année les conditions d'exécution du programme de l'article 702 dans son ensemble, en fixant notamment des limites générales aux sélecteurs pouvant être utilisées, les données qui doivent être effacées et les types de recherches qui peuvent être effectuées sur les données collectées en vrac. Il n'est pas censé autoriser le recours aux sélecteurs dans chaque affaire individuelle[98]. Un des problèmes inhérents à ce système tient à l'absence de suivi par un organe extérieur du respect des conditions énoncées par le FISC (comme indiqué *supra*, le processus d'affinage des sélecteurs est à la fois lent et extrêmement technique) et de l'application concrète des normes élevées de protection des données[99]. Le PCLOB a par conséquent recommandé au gouvernement de soumettre, en même temps que ses demandes annuelles un échantillon, choisi au hasard, de feuilles d'attribution à la NSA et à la CIA de tâches visant la recherche dans les données d'informations relatives à un citoyen américain, accompagnées de la documentation justificative. La taille de l'échantillon et la méthodologie doivent être approuvées par le tribunal du FISA. Une telle pratique permettrait au FISC de se faire une idée plus précise du respect dans la pratique des conditions qu'il énonce[100].

119. De plus, il convient de noter qu'une bonne partie des activités de ROEM des États-Unis échappe à la compétence du FISC. La surveillance des ressortissants étrangers en vertu de l'ordonnance de l'exécutif n° 12333 n'est pas soumise par le FISA au droit interne. En raison du manque général de transparence entourant le programme, personne n'a reconnu publiquement la quantité de données collectées en vertu de ladite ordonnance dans le cadre des activités de ROEM menées en vertu de programmes échappant au contrôle du FISC.

étrangère ou à un territoire étranger posant un risque pour la défense nationale et la politique de relations extérieures des États-Unis, voir 50 USC, paragraphe 1881a(a).

[97] Voir la description contenue dans le rapport du PCLOB sur l'article 702, p. 6. Voir également L. K. Donohue, « Section 702 and the Collection of International Telephone and Internet Content », 2014, http://scholarship.law.georgetown.edu/facpub/1355/, p. 30.

[98] Les États européens préfèrent généralement un système d'autorisation juridictionnelle préalable (voir, *supra*, la section VI). Comme indiqué *infra*, le tribunal suédois approuve les sélecteurs au cas par cas. Cependant, les besoins en renseignement des États-Unis sont énormes et le nombre de sélecteurs risque également d'être très élevé et en constante évolution. Il convient d'avoir à l'esprit que l'autorisation juridictionnelle n'est pas la panacée (rapport de 2007, paragraphes 205 à 216). Lorsqu'un tribunal doit approuver une multitude de sélecteurs et dispose de peu de temps pour ce faire, l'examen a toutes les chances d'être superficiel.

[99] *The Washington Post*, 16 août 2013.

[100] Rapport du PCLOB sur l'article 702, p. 141. Le système des États-Unis compte désormais une couche supplémentaire de contrôle externe, puisque le PCLOB est un organe indépendant créé par une loi au sein de la branche exécutive (voir Pub. L. n° 110-53, paragraphe 801(a), 121 Stat. 266, p. 352-358 (2007)). Cette dernière exige que l'ensemble des cinq membres du Conseil soit nommé par le président sur proposition du Sénat et avec l'aval de celui-ci pour des mandats décalés de six ans. Elle prévoit également que le conseil doit être composé de membres des deux principaux partis politiques : ni les Républicains ni les Démocrates ne peuvent compter plus de trois membres et, avant de nommer des membres n'appartenant pas à son parti, le président doit consulter le dirigeant de l'autre parti. Toutefois, les garde-fous en matière de protection de la vie privée instaurés par le FISA sont principalement conçus pour défendre les citoyens américains. Le contrôle exercé par le PCLOB vise essentiellement à assurer le respect de la législation (voir l'article 74), de sorte qu'il s'intéresse essentiellement au renforcement de la protection de la vie privée des citoyens américains. Il semble que le conseil nourrisse l'intention de s'intéresser bientôt à la question des garanties des droits des étrangers.

120. La Suède fournit un bon exemple de modèle combinant une autorisation juridictionnelle et un suivi effectué par des spécialistes. Un tribunal du renseignement militaire (Försvarsunderrättelsedomstolen ou UNDOM) a été établi de même qu'un organe de contrôle et de suivi appelé Inspection du renseignement militaire (Statens inspektion för försvarsunder-rättelseverksamheten ou SIUN)[101]. L'UNDOM se compose de deux anciens hauts magistrats et de six juges non professionnels (pour la plupart d'anciens hommes politiques ayant appartenu à différents partis). Les juges sont nommés par le gouvernement à l'issue d'un processus de recrutement ouvert au sein du Conseil judiciaire. Les anciens hommes politiques sont nommés par le gouvernement après consultation des partis représentés au parlement. L'UNDOM est donc un organe hybride. Doté d'un modeste greffe, il approuve les demandes émanant des répartiteurs de tâches en les assortissant de conditions supplémentaires et autorise également les demandes de tests émanant du service de ROEM (voir, *supra*, le paragraphe 77).

121. La SIUN se compose aussi de deux anciens hauts magistrats et de quatre anciens hommes politiques choisis parmi les différents partis et nommés de la même manière que les membres de l'UNDOM. Il s'agit donc également d'un organe hybride. Elle est assistée d'un petit secrétariat. Le gouvernement et d'autres organes nommément désignés peuvent confier la tâche au service de renseignement d'origine électromagnétique, le FRA (Försvarets radioanstalt), de produire des renseignements extérieurs sur un sujet donné. Cette décision ne fait l'objet d'aucun contrôle. Le FRA demande alors un mandat à l'UNDOM qui détermine les sélecteurs qui pourront être utilisés et les porteurs de signaux franchissant les frontières nationales (c'est-à-dire des câbles donnés en fonction de leur destination) qui pourront être surveillés. Les renseignements bruts sont alors livrés par les entreprises de télécommunication à un centre placé sous le contrôle physique de la SIUN qui vérifie que les conditions relatives aux porteurs des signaux – telles qu'elles ont été fixées par l'UNDOM – ont bien été respectées avant d'être transférées au FRA. La SIUN surveille ensuite l'application par le FRA des sélecteurs définis par l'UNDOM. S'il considère que les conditions fixées par ce dernier n'ont pas été respectées, il peut mettre fin à la recherche et ordonner la destruction de tout le matériel éventuellement collecté.

122. Le système mis en place relève donc davantage d'un contrôle que d'une supervision, même si la SIUN assume à la fois les fonctions de supervision et de traitement des plaintes (voir *infra*) dans la mesure où elle vérifie si le FRA respecte les exigences relatives à la gestion des données à caractère personnel[102]. Le modèle suédois n'est en place que depuis 2009, de sorte qu'il est relativement nouveau. Il comporte certains avantages majeurs inhérents aux capacités techniques mobilisées, à son caractère hybride (juridictionnel/politique) et au fait que ses membres sont élus après consultation de tous les partis. Cela dit, il n'est pas dépourvu de défauts, notamment sous l'angle d'un manque de compétences spécialisées. L'acquisition et la conservation de telles compétences constituent en effet un processus lent qui suppose nécessairement un personnel stable doté du savoir requis afin de garantir l'intégrité du contrôle : une ambition d'autant plus difficile à réaliser qu'il est souvent malaisé d'offrir un plan de carrière satisfaisant à de tels professionnels dans le cadre d'organismes administratifs aussi petits.

---

[101] Voir la loi sur le renseignement d'origine électromagnétique (2008:717) telle que modifiée par la Prop. 2008/09:201, Förstärkt integritetsskydd vid signalspaning (Protection renforcée de l'intégrité dans l'interception du signal), 20 mai 2009. Des règles plus détaillées figurent dans l'ordonnance contenant des instructions à l'intention de la SIUN, 2009:969. Les règles élémentaires que le FRA et le service de renseignement militaire doivent tous deux respecter sous le contrôle de la SIUN sont énoncées dans la loi sur le renseignement militaire (2000:130).

[102] Loi (2007:259) sur le traitement des données à caractère personnel dans le cadre des activités de renseignement et de test du FRA. L'organe de contrôle, à savoir la SIUN, a été lui-même évalué par la Cour des comptes de la Suède qui a dressé un bilan globalement positif de son activité (RiR 2015:2, Kontrollen av försvarsunderrättelseverksamheten). L'Inspection du renseignement militaire supervise également les données à caractère personnel conservées par le FRA.

X. Contrôle par des organes spécialisés

123. La distinction entre les organes parlementaires, juridictionnels et spécialisés n'est pas nette et les choses évoluent rapidement dans ce domaine. Les modèles suédois et allemand peuvent être perçus comme réunissant ces trois aspects, dans la mesure où les entités concernées exercent également des fonctions de contrôle. En revanche, les organes de surveillance belge, néerlandais, norvégien et – depuis 2013 – danois sont davantage des entités de supervision spécialisées n'exerçant pas de fonction de contrôle[103]. Tous ces organes disposent d'un mandat analogue et de larges pouvoirs de supervision assez semblables (y compris sur la surveillance stratégique exercée par les organes qu'ils sont censés contrôler). Si l'on prend le modèle néerlandais comme exemple : la Commission de contrôle des services de renseignement et de sécurité (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten ou CTIVD) est établie par une loi (loi de 2002 sur les services de renseignement et de sécurité ou ISS) et son but principal consiste à vérifier que ladite loi – censée régir les activités à la fois du GIIS (Service général de renseignement et de sécurité) et du DISS (Service de renseignement, de défense et de sécurité) – est correctement mise en œuvre, y compris sous l'angle du respect du principe de proportionnalité. Sur les trois membres que compte cet organe, deux doivent être des juristes (article 65.4). La CTIVD est assistée d'un secrétariat et, actuellement, de six enquêteurs. Elle s'acquitte de sa tâche de supervision de deux façons : elle peut mener des enquêtes approfondies débouchant sur la publication d'un rapport d'examen qui est rendu public et elle peut également suivre un certain nombre d'activités déployées par les services. Elle dispose de pouvoirs légaux étendus de manière à pouvoir s'acquitter de sa principale tâche de contrôle (articles 74 à 77 de l'ISS de 2002). Elle a accès à toutes les informations classifiées pertinentes détenues par les services et peut donc contrôler à la fois l'acquisition des renseignements et leur diffusion, y compris ceux en provenance ou à destination de services de pays amis (en d'autres termes, la règle dite « de la maîtrise de l'information par son auteur » ne s'applique pas).

124. La CTIVD (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten ou CTIVD) a publié un nombre de rapports détaillés sur la surveillance stratégique[104]. Le premier pose la question de savoir si les pratiques existantes sont conformes à la loi ; il critique également l'absence de documentation justifiant certaines opérations de collecte de renseignements d'origine électromagnétique. Le second rapport constitue une analyse en profondeur de la manière dont les services de sécurité et de renseignement néerlandais acquièrent et utilisent des données à partir des communications personnelles et les échangent avec des services étrangers.

125. Pour conclure sur la question des organes de contrôle spécialisés, il paraît essentiel de souligner que ces entités doivent pouvoir accéder librement aux informations personnelles contenues dans les bases de données du service de ROEM pour pouvoir servir utilement de garde-fous[105]. Le principe de la maîtrise de l'information par son auteur

[103] Pour la réforme entreprise au Danemark, voir la loi 162, 2013, et ses travaux préparatoires (Betaenkning om PET og FE, n° 1529, 2012). Comme indiqué *supra*, au sein du système américain, le PCLOB exerce désormais une fonction de contrôle général analogue sur le ROEM militaire.

[104] CTIVD, rapport n° 28, *op cit*. "The use of Sigint by DISS" et CTIVD, rapport n° 38 : « The processing of telecommunications data by GISS and DISS », http://english.ctivd.nl/ (en anglais).

[105] Voir en particulier le paragraphe 87 du rapport de 2007 « [à] moins d'être en situation de mener une "seconde évaluation" raisonnablement bien informée, un organe de supervision n'est pas un véritable garde-fou […] », ainsi que son paragraphe 237 « [g]ardant à l'esprit l'importance cruciale des banques de données pour le travail d'une agence de sécurité, et la distinction déjà mentionnée entre les renseignements de sécurité et les informations "solides" […] il est impératif qu'un organe de supervision de ce type existe dans chaque État et qu'il dispose de pouvoirs suffisants, dans la loi et la pratique, pour exercer de manière satisfaisante les fonctions de contrôle ».

ne saurait s'appliquer à un organe de contrôle. Bien qu'un organe spécialisé se contente principalement, dans le cadre de cette activité, de vérifier que les propres procédures du service de ROEM (en matière de minimisation, etc.) fonctionnent correctement, il ne peut s'acquitter de cette tâche qu'en procédant à des contrôles par sondage et à une étude thématique des vraies données. Par conséquent, il doit disposer de ses propres capacités résiduelles en matière d'enquête et, de préférence, pouvoir accéder directement (comme c'est le cas des organes de contrôle néerlandais et suédois) aux banques de données abritant des informations à caractère personnel. Il est possible, pour mieux faire ressortir les problèmes potentiels, d'obliger le service de ROEM à fournir de sa propre initiative à l'organe de contrôle certaines catégories de données particulièrement sensibles[106]. Les modalités de l'interrogation des données collectées en vrac et des moyens ou de l'objet de la diffusion des renseignements tirés desdites données doivent également faire l'objet d'un contrôle. La tendance est actuellement à des « centres de fusion » destinés à recevoir les données intéressant la sécurité intérieure. Une telle pratique peut de toute évidence largement accroître la taille du groupe ayant accès aux données à caractère personnel obtenues dans le cadre d'activités de ROEM. On peut en dire autant du recours à des sous-traitants privés. La coexistence de contrôles laxistes sur l'acquisition et de règles vagues de minimisation et d'accès aux données représente manifestement une combinaison dangereuse. Pourtant, même des contrôles stricts sur les modalités de l'acquisition et de la minimisation se révéleront insuffisants s'ils ne sont pas assortis d'un accès facile à la base de données.

XI. Mécanismes de traitement des plaintes

126. Comme indiqué *supra*, la législation prévoit généralement que la cible d'une surveillance ordinaire doit recevoir notification une fois l'opération terminée et à condition que cette notification ne porte pas atteinte à la confidentialité des méthodes utilisées ou d'opérations en cours. Concernant les opérations de sécurité interne, la non-notification semble être la règle[107]. Certains systèmes de surveillance stratégique prévoient également une notification dès lors que les sélecteurs choisis sont directement associés à une personne physique donnée. Des dispositions en ce sens figurent à l'article 11.*a* de la loi suédoise sur le renseignement d'origine électromagnétique et dans la législation allemande (loi G10, article 12, bien que cette mesure vise uniquement les ressortissants allemands ou les personnes résidant en Allemagne). Dans les deux cas, il est prévu des exceptions lorsque la notification pourrait porter atteinte à la sécurité. En vertu de la législation allemande, la commission G10 doit approuver la non-notification au cas par cas, .de sorte que l'exigence de notification, même si elle n'aboutit que rarement à une véritable notification, peut s'avérer utile dans la mesure où elle tend à limiter l'utilisation excessive (puisque le service de surveillance stratégique sait parfaitement que chaque fois qu'il surveille les communications d'un ressortissant ou d'un résident, il devra en informer l'organe de contrôle et convaincre celui-ci qu'il a de bonnes raisons de notifier la surveillance à la personne concernée). Les chiffres relatifs aux cas de notification (et de non-notification), s'ils étaient publiés, pourraient également servir à apaiser les craintes du public concernant l'échelle de la surveillance[108].

---

[106] Voir, par exemple, les règles allemandes relatives aux obligations positives de reddition de comptes concernant les données relatives au cœur de la protection de la vie privée.

[107] Selon l'expérience accumulée par la CTIVD, il n'y a jamais de notification dans le cadre d'une surveillance exercée par le service de ROEM, rapport du CTIVD n° 24, *« on the performance of GISS of its obligation to notify »,,* p. 23.

[108] L'Allemagne publie chaque année le nombre d'affaires ayant donné lieu à une notification et d'affaires n'ayant pas donné lieu à une notification, voir le Deutscher Bundestag Drucksache 18/3709, 8 janvier 2015, p. 5 et 8.

127. La CEDH prévoit que l'État doit offrir un moyen de recours effectif à tout justiciable alléguant une violation de ses droits. Pour qu'un recours soit considéré comme effectif, certaines conditions doivent être respectées[109]. L'article 8 de la Convention n'impose pas expressément qu'il soit notifié à une personne qu'elle a fait l'objet d'une surveillance stratégique. En effet, l'absence de notification peut être compensée par la mise en place d'une procédure générale de traitement des plaintes gérée par un organe de contrôle indépendant. L'absence de notification ne doit pas empêcher de déposer plainte. À titre d'exemple d'une procédure générale de traitement des plaintes, on peut citer l'article 10.*a* de la loi suédoise sur le renseignement d'origine électromagnétique, laquelle prévoit ceci : « L'autorité de contrôle est tenue, à la demande d'un individu, de vérifier si des messages de l'intéressé ont été obtenus en liaison avec des activités de ROEM menées dans le cadre de la présente loi et, le cas échéant, si les processus de collecte et de traitement des données étaient conformes à la législation. L'autorité de contrôle doit notifier à l'intéressé qu'elle a procédé à la vérification. Cette voie de recours ne se limite pas explicitement aux seuls ressortissants suédois. »[110]

XII. Remarques de conclusion

128. Le renseignement d'origine électromagnétique pose un sérieux risque potentiel d'ingérence dans la vie privée et dans l'exercice d'autres droits individuels. Appréhender la surveillance stratégique uniquement par le prisme de la protection de la vie privée ne permet pas de mesurer toute l'ampleur de ce risque. À la différence de la restitution (rendition) qui constitue un préjudice clair, immédiat et individuel, les dommages potentiels pour la société associés à des activités de ROEM insuffisamment réglementées et contrôlées sont à la fois plus diffus et plus durables. La situation actuelle pourrait faire peser des obligations concurrentes, voire antagonistes (inhérentes le plus souvent aux avantages/inconvénients respectifs de la divulgation et de la protection des données) sur les entreprises de télécommunication et favoriser le contournement des procédures plus strictes en matière de surveillance intérieure. Il apparaît donc d'autant plus nécessaire de se mettre d'accord sur des normes internationales minimales en matière de protection de la vie privée.

129. Le renseignement d'origine électromagnétique peut être réglementé de manière laxiste, c'est-à-dire qu'un grand nombre de personnes seront prises dans les mailles du filet de la surveillance, ou bien de manière relativement stricte, c'est-à-dire que les cas réels d'ingérence dans la vie privée ou d'autres droits personnels d'un individu seront plus rares. Les États parties à la CEDH, quant à eux, doivent de toute façon réglementer les principaux éléments du ROEM au moyen d'une loi. Le parlement national doit se voir conférer la possibilité réelle de comprendre ces questions et d'assurer les équilibres requis. Toutefois, les États européens ne devraient pas se contenter de satisfaire les normes de qualité de la loi énoncées dans la CEDH, dans la mesure où seuls de solides mécanismes de contrôle et de supervision indépendants pourront apaiser les craintes du public concernant les risques d'un recours abusif au renseignement d'origine électromagnétique.

---

[109] Voir *mutatis mutandis* « Lignes directrices du Comité des Ministres du Conseil de l'Europe pour éliminer l'impunité pour les violations graves des droits de l'homme », 30 mars 2011 : un document selon lequel les critères d'une enquête effective sont l'adéquation, l'approfondissement, l'impartialité et l'indépendance, la promptitude et la publicité.

[110] On peut également noter que la CTIVD fait office d'organe consultatif interne en matière de traitement des plaintes. Son avis est envoyé au ministre qui rend ensuite une décision en toute indépendance. Lorsque l'intéressé ne suit pas l'avis du conseil, il doit joindre celui-ci au courrier faisant part de sa décision au plaignant. Si ce dernier s'oppose à la décision du ministre, il peut de nouveau déposer plainte, cette fois-ci auprès de l'ombudsman national. La CTIVD traite 10 à 15 plaintes chaque année, dont un tiers environ est généralement infondé et une minorité fondée ou partiellement fondée. Voir, par exemple, le rapport annuel 2013-2014 de la CTIVD, p. 9 à 11.

Glossaire

Agence des renseignements électromagnétiques	Agence des renseignements électromagnétiques engagée dans la collecte et l'analyse des ROEM, soit comme seul but soit en tant qu'un de ses objectifs.
BND	*Bundesnachrichtendienstes :* Agence fédérale allemande du renseignement extérieur.
Commission G10	Organisme de surveillance indépendant pour l'interception de communications en Allemagne, établi par la Loi fédérale limitant la confidentialité de la correspondance, de la poste et des télécommunications (énoncé par l'article 10 de la Constitution fédérale, et par ce qu'on appelle la Loi G10).
CTIVD	*De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten:* Commission de contrôle des services de renseignement et de sécurité
Communication via un câble (*cable-borne communication**)***	Communication via un câble (par exemple fibre optique ou câble en cuivre).
Données de contenu (*Content data*)	Contenu d'une télécommunication ou de données stockées, par exemple les mots écrits dans un e-mail ou prononcé pendant un appel téléphonique.
Données en vrac (*Bulk data*)	Très grandes quantités de données de communication (données et métadonnées) collectées par des processus automatisés.
Enchaînement des contacts (*Contact chaining*)	Processus d'identification des modes de communication de métadonnées, qui consiste généralement à vérifier si les numéros de téléphone suspects identifiés précédemment sont en contact avec d'autres numéros, et ensuite si ces numéros sont à leur tour en contact avec d'autres numéros.
FAI *(ISP)*	Fournisseur de services internet.
FRA	*Försvarets Radio Anstalt :* Agence suédoise de renseignements électromagnétiques.
GCHQ	*UK Government Communications Headquarters :* Agence de renseignements électromagnétiques du Royaume-Uni.
Métadonnées *(metadata)*	«Données sur les données» : dans le contexte des télécommunications, sont généralement considérées comme telles toutes les données qui ne font pas partie du contenu de la communication, par exemple les numéros appelés, la durée de l'appel, l'emplacement de l'appelant et du destinataire, etc. Les métadonnées peuvent être analysées en rapport avec des schémas de communications.
Minimisation	Suppression par les analystes humains de matériel non pertinent pour une enquête, recueilli dans le cadre d'une interception de télécommunications.
NSA	*National Security Agency :* Agence de renseignements électromagnétiques des États-Unis.
PCLOB	*Privacy and Civil Liberties Oversight Board :* organisme indépendant de surveillance des SIGINT nommé par l'exécutif pour les questions de la vie privée et des libertés civiles aux États-Unis.
PkGr	*Parlamentarisches Kontrollgremium :* Comité de contrôle parlementaire allemand.

ROEM *(SIGINT - Signals Intelligence)*	Renseignements d'origine électromagnétique : terme collectif qui se réfère aux moyens et méthodes pour l'interception et l'analyse des communications émises par la radio (y compris par satellite et par téléphone cellulaire) et par câble.
Sélecteur	Terme utilisé soit pour filtrer les données en vrac en temps réel, soit pour interroger des données recueillies en vrac. Celles-ci peuvent être liées à la langue, aux personnes, aux mots-clés concernant le contenu, aux voies de communication et à d'autres données techniques, ou à tout cela.
SIUN	*Statens inspektion för försvarsunderrättelseverksamheten*: Inspection du renseignement militaire de la Suède.
Surveillance ciblée	Police ou agence de renseignement chargée d'une surveillance des individus ou des groupes lancée après qu'un organisme indépendant a constaté qu'il existe des faits concrets, et un soupçon raisonnable, indiquant que des individus ou des groupes sont impliqués dans des crimes ou des menaces pour la sécurité nationale.
Surveillance stratégique	Collection de très grandes quantités de données électroniques et de métadonnées qui sont ensuite soumises à une analyse par l'ordinateur à l'aide de sélecteurs.
UNDOM	*Underrättelsedomstolen:* Tribunal suédois de renseignement militaire.