Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'Union européenne

Résumé

L'article 7 de la Charte des droits fondamentaux de l'Union européenne garantit à toute personne dans l'Union européenne (UE) le respect de sa vie privée et familiale, tandis que l'article 8 garantit le droit à la protection des données à caractère personnel la concernant. Il exige que ces données soient traitées loyalement et à des fins déterminées. Il garantit à toute personne le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Il prévoit aussi qu'une autorité indépendante doit veiller au respect de ce droit. L'article 47 garantit à toute personne le droit à un recours effectif, notamment que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable.

Lorsque les médias du monde entier commencèrent à publier les « documents d'Edward Snowden » en juin 2013, l'existence de programmes mondiaux de surveillance massive par les services de renseignement a été révélée. Les documents divulgués par Edward Snowden n'étaient pas les premiers à faire allusion à la surveillance des communications à grande échelle mise en place au lendemain des attentats du 11 septembre 2001. Cependant, ces révélations ont pris une ampleur sans précédent qui pourrait potentiellement avoir une incidence sur la vie privée des personnes à travers le monde. La surveillance ne vise plus seulement les secrets d'État ou les secrets d'affaires, mais permet d'intercepter les communications des personnes à grande échelle. Elle constitue une ingérence dans le respect de la vie privée et familiale des personnes et dans le droit à la protection des données – tous deux garantis au niveau de l'Union européenne par la Charte des droits fondamentaux de l'Union européenne (la Charte). C'est pourquoi l'UE et ses États membres se doivent de les protéger, y compris dans le contexte de la surveillance, et d'offrir aux victimes des voies de recours qui leur permettent de contester une surveillance illégale.

« Une telle surveillance massive et non ciblée est disproportionnée par nature et constitue une ingérence injustifiée dans les droits garantis par les articles 7 et 8 de la Charte. »
(CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, Conclusions de l'avocat général, 23 septembre 2015)

Ces révélations ont provoqué une série de réactions. Dans la communauté du renseignement, en particulier parmi les organes spécialisés chargés de contrôler les services de renseignement, des enquêtes et des rapports portant spécifiquement sur les révélations d'Edward Snowden ont examiné leurs implications. Les institutions de l'UE ont vivement réagi. La Commission européenne, le Conseil de l'Union européenne et le Parlement européen ont tous commenté les révélations, ont fait part de leur préoccupation concernant les programmes de surveillance massive, ont demandé des précisions aux autorités américaines et se sont employés à « rétablir la confiance » dans les relations entre l'Union européenne et les États-Unis. Bien qu'il soit trop tôt pour évaluer toutes les incidences des révélations d'Edward Snowden, des enquêtes réalisées dans plusieurs États membres de l'UE après l'affaire Snowden ont conclu à la nécessité de réformer les cadres

juridiques nationaux existants. C'est également ce qu'a souligné le Parlement européen dans sa résolution de mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens de l'UE et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI), P7_TA (2014)0230), en lançant un *Habeas Corpus numérique européen*.

« Les révélations d'Edward Snowden nous ont donné une chance de réagir. J'espère que nous transformerons ces réactions en quelque chose de positif et de durable lors de la prochaine législature de ce Parlement, en une législation sur la protection des données dont nous pourrions tous être fiers »
(Claude Moraes, député européen, rapporteur sur l'enquête du Parlement européen concernant la NSA, Communiqué de presse, 12 mars 2014)

Panorama des cadres juridiques des États membres de l'UE en matière de surveillance

En avril 2014, le Parlement européen a demandé à l'Agence des droits fondamentaux de l'Union européenne (FRA) « d'effectuer des recherches approfondies sur la protection des droits fondamentaux dans le contexte de la surveillance ». C'est ce que la FRA a effectué, en établissant un panorama du droit des 28 États membres de l'UE en matière de surveillance et en donnant une vue d'ensemble des droits fondamentaux en la matière. La FRA a porté son attention sur les mécanismes de contrôle et sur les voies de recours offertes aux personnes qui affirment avoir été victimes d'une violation de leur droit à la vie privée.

Les recherches juridiques de la FRA ne portent pas sur les techniques de renseignement proprement dites. La FRA examine comment les cadres juridiques actuels permettent d'avoir recours à ces techniques, et étudie le rôle essentiel que jouent les organes spécialisés dans le contrôle des travaux des services de renseignement. Par ailleurs, la FRA analyse dans quelle mesure les garanties en question contribuent à protéger la vie privée et les données personnelles dans les 28 États membres de l'UE.

Le rapport de la FRA utilise le terme générique « services de renseignement » pour se référer aux services spécialisés dans le renseignement intérieur qui se concentre sur les menaces nationales et ceux spécialisés dans le renseignement extérieur ayant un mandat international.

Le présent résumé présente les principales conclusions des recherches la FRA, qui sont intégralement publiées dans le rapport intitulé *Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'UE - Panorama du droit des États membres* (voir les Informations supplémentaires).

Collecte de données et champ de la recherche

Aux fins de la présente étude, la FRA a passé en revue les cadres juridiques des 28 États membres de l'UE en matière de surveillance, en analysant les lois et les normes pertinentes en matière de droits fondamentaux, pour pouvoir présenter une analyse comparée sur le droit du renseignement dans l'UE.

Sur la base des réponses fournies par Franet, le réseau de recherche multidisciplinaire de la FRA, l'agence a collecté des données et des informations au moyen d'une recherche documentaire effectuée dans les 28 États membres. Des informations complémentaires ont été rassemblées grâce à des échanges avec des partenaires clés, dont un certain nombre d'agents nationaux de liaison de la FRA, des organes spécialisés et des experts indépendants. Les conclusions reposent aussi sur des rapports et des publications existants destinés à aider les législateurs nationaux à mettre en place des cadres juridiques pour les services de renseignement et leur contrôle démocratique.

Un second rapport socio-juridique, renfermant des avis de la FRA et reposant sur des recherches empiriques, sera publié ultérieurement, et développera davantage les conclusions présentées ici.

Protection des droits fondamentaux et droit de l'UE

« La vérité est incontestablement que l'utilisation de la technologie de surveillance de masse élimine en fait purement et simplement le droit au secret des communications sur l'Internet. »
(*Nations Unies (ONU), Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (2014)*, Quatrième rapport annuel présenté à l'Assemblée générale, *A/69/397, 23 septembre 2014*)

Les États membres de l'UE sont tous liés par les normes internationales minimales élaborées par les Nations Unies (ONU) en matière de droits de l'homme, qui revêtent un caractère universel, comme la Résolution du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique (Doc. A/HRC/28/L.27, 24 mars 2015). Plusieurs organes d'experts et organes créés en vertu de traités des Nations Unies ont condamné les pratiques de surveillance de masse après les révélations d'Edward Snowden. Les normes du Conseil de l'Europe, y compris la jurisprudence de la Cour européenne des droits de l'homme (CouEDH), énoncent aussi des normes minimales. En outre, le droit de l'UE, tel qu'interprété par la Cour de justice de l'Union européenne (CJUE), est pertinent. Enfin, dans un domaine peu règlementé au niveau national – mis à part le droit international des droits de l'homme – des mesures d'autorégulation et la soft law jouent un rôle important.

Le rapport porte sur les droits au respect de la vie privée et à la protection des données, qui sont consacrés aux articles 7 et 8 de la Charte. Le droit à la protection des données est prévu dans le droit primaire et le droit dérivé de l'UE, ce qui permet de garantir que, dans leur domaine d'application respectif, les données à caractère personnel sont traitées de manière légale et uniquement dans la mesure nécessaire à la réalisation du but légitime poursuivi. Ces droits s'appliquent à toutes les personnes, qu'elles soient citoyennes de l'UE ou ressortissantes de pays tiers. En vertu de l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice de ce droit doit être nécessaire et proportionnée, répondre effectivement à des objectifs d'intérêt général reconnus par l'Union, prévue par la loi, et respecter le contenu essentiel des dits droits.

Malgré l'existence de lignes directrices internationales, il n'existe pas d'interprétation commune de la notion de « sécurité nationale » dans l'UE. Ni la législation de l'UE ni la jurisprudence de la CJUE ne définissent cette notion, bien que la CJUE ait précisé que les exceptions aux droits fondamentaux doivent être interprétées de manière étroite et justifiées.

Cette définition floue de la « sécurité nationale » a des répercussions sur l'applicabilité du droit de l'UE. Aux termes de l'article 4, paragraphe 2, du Traité sur l'Union européenne, « la sécurité nationale reste de la seule responsabilité de chaque État membre ». Cela ne signifie pas que la dérogation de la « sécurité nationale » rend le droit de l'UE entièrement inapplicable. L'interprétation de la notion de « sécurité nationale » au niveau des États membres et les modalités d'exécution des programmes de surveillance peuvent être évaluées par les institutions de l'UE, en particulier la CJUE.

Types de surveillance : ciblée et non ciblée

Les recherches de la FRA examinent comment sont organisées la surveillance ciblée et la surveillance non ciblée en droit des États membres de l'UE.

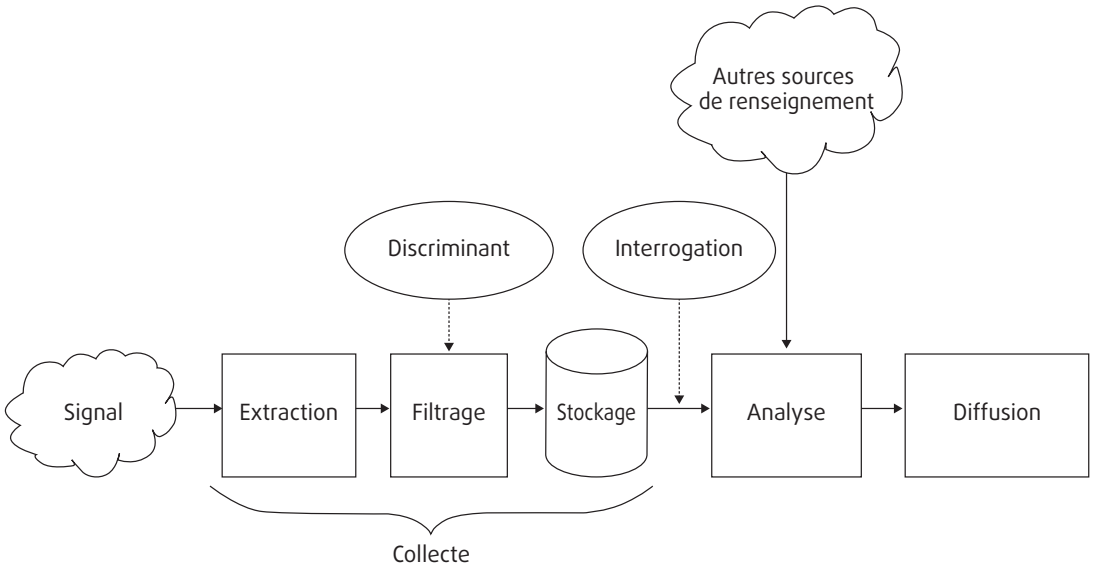
Le Comité néerlandais de surveillance des services de renseignement et de sécurité (CTIVD) définit la surveillance ciblée et non ciblée de la manière suivante :

- l'interception ciblée désigne une situation dans laquelle il est possible de préciser à l'avance la personne, l'organisation ou la caractéristique technique ciblée par la collecte de données ;
- l'interception non ciblée désigne une situation dans laquelle il n'est pas possible de préciser à l'avance la personne, l'organisation ou la caractéristique technique ciblée par la collecte de données.

CTIVD, *Annual report 2013-2014*, La Haye, 31 mars 2014, p. 45–46

Le volume considérable de données collectées au moyen des programmes de surveillance rendus publics, tels que PRISM, Xkeyscore et Upstream, a suscité des réactions à grande échelle. La « surveillance de masse » (souvent comprise comme étant non ciblée) implique la collecte de volumes de données très vastes par rapport aux données qui sont collectées à l'aide de méthodes de surveillance traditionnelles, secrètes (ciblées), comme les écoutes téléphoniques. Ces dernières reposent sur le soupçon préalable portant sur un individu ou une organisation spécifique. Ce type de surveillance est observé dans les États membres de l'UE

Figure : Modèle conceptuel du renseignement électromagnétique



Source : États-Unis, Conseil national de la recherche (2015), p. 28

et reconnu par leur législation. L'immense majorité des cadres juridiques des États membres de l'UE ne règlemente pas et ne mentionne même pas la « surveillance de masse » en tant que telle. Seuls quelques États membres de l'UE ont adopté une législation détaillée sur le renseignement d'origine technique (SIGINT, *signals intelligence*), qui est le terme générique utilisé pour décrire l'interception par les services de renseignement de signaux provenant de diverses sources. L'étude de la FRA emploie le terme « renseignements d'origine électromagnétique » dans son analyse.

Initialement, le SIGINT relève du domaine militaire. Il renvoie à la collecte d'informations automatisée au moyen de l'interception et de la collecte de données numériques liées à l'activité de renseignement. La figure suivante indique que les signaux collectés sont filtrés au moyen de sélecteurs et de discriminants – un ensemble de paramètres utilisés dans le processus de filtrage, *soit a priori* ou de manière dynamique, pour définir les critères qui détermineront quelles sont les données qui doivent être stockées pour obtenir l'information pertinente (par exemple, « toutes les adresses de courrier électronique utilisées dans les communications avec le Yémen »).

Selon le Conseil national de la recherche des États-Unis, le terme « renseignement d'origine électromagnétique » englobe toutes les données stockées sur un appareil électronique. Pour la Commission de Venise, le SIGINT 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.

Selon l'analyse de la FRA portant sur les cadres juridiques qui régissent les méthodes de surveillance des services de renseignement, les lois de cinq États membres de l'UE (Allemagne, France, Pays-Bas, Royaume-Uni et Suède) détaillent les conditions dans lesquelles il est possible d'avoir recours à la surveillance ciblée et non ciblée, comme les renseignements d'origine électromagnétique. Les lois des autres États membres ne précisent pas suffisamment ces conditions, ce qui ne permet pas de procéder à une analyse juridique des procédures exactes en place sur la collecte de renseignements d'origine électromagnétique. Même si dans ces pays les lois ne mentionnent pas explicitement le SIGINT, il peut cependant être utilisé. Toutefois, étant donné que la pratique est prescrite uniquement dans des règlements qui ne sont pas publiés, l'analyse des cadres juridiques applicables n'apportera aucun éclaircissement sur la question.

Points clés

Services de renseignement et lois relatives à la surveillance

Objectif et structure des services de renseignement

Dans les sociétés démocratiques, le principal objectif des services de renseignement est de protéger la sécurité nationale et les valeurs fondamentales d'une société ouverte en utilisant des techniques de renseignement secrètes. L'organisation de la communauté du renseignement dans chaque État membre de l'UE est étroitement liée à des développements historiques propres au pays en question, et n'est pas nécessairement influencée par les droits fondamentaux. Les services de renseignement sont donc organisés de façons très différentes à travers l'UE. Dans certains États membres, deux services de renseignement ont été établis, tandis que dans d'autres, il y en a cinq ou six.

- Presque tous les États membres de l'UE ont mis en place au moins deux services de renseignement différents, le premier, civil, et le second, militaire. Les services de renseignement militaire ne sont pas abordés dans le cadre du présent rapport. Les services de renseignement civil sont généralement subordonnés au ministère de l'Intérieur, et parfois au premier ministre ou au président.

- Dans certains États membres, les services civils sont subdivisés en deux services : le premier a un mandat national et le second un mandat international. En outre, certains États membres ont confié les techniques de renseignement à des unités spécialisées dans une menace en particulier, comme le crime organisé, la corruption ou la lutte contre le terrorisme.

Protection de la sécurité nationale

L'étude de la FRA analyse la notion de « sécurité nationale » compte tenu du mandat des services de renseignement et des techniques de surveillance qu'ils sont susceptibles de mettre en œuvre. Là encore, les résultats révèlent une grande diversité parmi les États membres de l'UE.

- L'objectif principal des services de renseignement est de protéger la sécurité nationale, mais cette notion n'est pas harmonisée dans les États membres de l'UE. L'étendue de la sécurité nationale est rarement définie, et des termes similaires sont parfois employés. D'autres États membres n'emploient pas le terme de « sécurité nationale », mais font référence à la « sécurité intérieure » et/ou la « sécurité extérieure », ou encore la « sécurité de l'État ».

- Le champ d'action des services de renseignement (à savoir leur mandat) n'est pas le même dans tous les États membres de l'UE. Outre les domaines plus traditionnels, les mandats de certains services de renseignement comprennent aussi le crime organisé et la cybercriminalité. Ces termes ne sont pas définis de manière harmonieuse.

Législation relative à la surveillance

Il est parfois difficile d'établir la limite entre les missions des forces de l'ordre et celles des services de renseignement. Toute extension des missions doit être dûment justifiée comme étant nécessaire à la protection de l'État, qui est la raison qui sous-tend la mise en place de services de renseignement.

- La plupart des cadres juridiques des États membres régissent uniquement la surveillance ciblée, soit de personnes soit de groupes/organisations bien précis. En plus de tenir compte de la surveillance ciblée, cinq États membres ont adopté des lois détaillées sur les conditions d'utilisation des renseignements d'origine électromagnétique.

- Au vu des standards applicables en matière de droits de l'homme, les droits nationaux manquent de précision au sujet des catégories de personnes et de l'éventail d'activités qui peuvent faire l'objet d'une technique de renseignement.

- Les services de renseignement sont réglementés par la loi dans la grande majorité des États membres (26 sur 28). Des dispositions juridiques régissent l'organisation et le fonctionnement des services de renseignement nationaux. La constitution d'un État membre interdit à ses services de renseignement de mener des opérations de surveillance. Un autre État membre est sur le

point d'adopter une législation qui réglementera les pratiques de ses services de renseignement.

- L'analyse de la FRA indique que la base juridique qui établit le mandat et les pouvoirs des services de renseignement nationaux varie selon les États membres de l'UE : il peut s'agir d'un instrument juridique unique régissant l'organisation et les moyens des services, ou de cadres juridiques complexes qui consistent en plusieurs lois et règlements régissant les aspects spécifiques de leur mandat, leur organisation, leurs compétences et moyens.

- La plupart des États membres ont adopté deux lois distinctes aux fins de l'organisation des travaux des services de renseignement : la première concerne le mandat et l'organisation du service, la deuxième porte sur les moyens d'action et les conditions de leur utilisation.

- La majorité des États membres de l'UE (23 sur 28) ont séparé les services de renseignement des services répressifs. Deux États membres se sont récemment détournés de systèmes en vert u desquels les services de renseignement relevaient de la police ou des services répressifs similaires.

Contrôle des services de renseignement

L'analyse de la FRA passe en revue les mécanismes relatifs à l'obligation de rendre compte des opérations de surveillance menées par les services de renseignement. Elle décrit notamment comment les États membres de l'UE ont mis en place des mécanismes de contrôle. Le contrôle est un moyen d'assurer que l'obligation de rendre compte des décisions et des opérations des services de renseignement soit respectée. Selon des experts, le contrôle vise à éviter les abus de pouvoir, à légitimer l'exercice de pouvoirs d'ingérence et à obtenir de meilleurs résultats après l'évaluation d'actions spécifiques. Un rapport de la Commission de Venise et d'autres études universitaires laissent transparaitre un consensus général selon lequel le contrôle devrait combiner :

- un contrôle exécutif ;
- un contrôle parlementaire ;
- un contrôle par des organes d'experts ;
- un contrôle juridictionnel.

Contrôle exécutif et coordination entre les organes de contrôle

Le pouvoir exécutif peut contrôler les services de renseignement de diverses manières : en précisant leurs politiques et leurs priorités stratégiques ou en établissant des lignes directrices ; en nommant et/ou en désignant les dirigeants du service ; en formulant le budget qui sera ensuite voté par le parlement ; ou en approuvant la coopération avec d'autres services. L'exécutif joue aussi un rôle décisif lorsqu'il s'agit d'autoriser des mesures de surveillance dans quelques États membres.

Un contrôle efficace exige une bonne coordination entre les divers organes de contrôle pour s'assurer que tous les aspects des travaux des services de renseignement soient couverts. Si les organes de contrôle n'ont pas une compréhension claire et approfondie des travaux de la communauté nationale de renseignement dans son ensemble, des lacunes apparaîtront, et l'efficacité du système de contrôle dans son ensemble en pâtira.

- La diversité des systèmes politiques et juridiques parmi les États membres de l'UE s'est traduite par une grande diversité d'organes qui contrôlent les services de renseignement. Les États membres de l'UE sont dotés de systèmes de contrôle très différents. Bien que de bonnes pratiques soient issues des systèmes en place, une réforme juridique destinée à renforcer le pouvoir des organes de contrôle serait bénéfique dans certains domaines.

- Les différents organes de contrôle sont dotés d'un large éventail de pouvoirs, dont l'étendue varie également.

- Sept États membres disposent de systèmes de contrôle qui combinent le pouvoir exécutif, le parlement, le pouvoir juridictionnel (au moyen d'une approbation *ex ante*) et d'organes d'experts. Cependant, il ne s'agit pas des pays qui disposent de cadres juridiques autorisant la collecte de renseignements d'origine électromagnétique.

- Un contrôle efficace ne requiert pas nécessairement d'avoir recours aux quatre types de mécanismes de contrôle. Le contrôle est efficace dès lors que les organes en place se complètent et qu'ils forment un système solide capable d'évaluer si les services de renseignement s'acquittent correctement de leur mandat. Tel sera le cas si les pouvoirs de contrôle s'appliquent à tous les domaines d'activité des services de renseignement. Cependant, lorsque le mandat en lui-même n'est pas clair ou qu'il n'est pas suffisamment détaillé, les organes de contrôle ne seront pas en mesure d'exercer une quelconque influence.

- Il est essentiel que les organes de contrôle aient accès aux informations et documents. Bien que les informations collectées par les services de renseignement soient sensibles, et que des garanties doivent préciser qu'elles seront traitées en conséquence, les organes de contrôle ne peuvent pas mener à bien leur mission sans avoir eu accès à toutes les informations pertinentes. Il semblerait toutefois que ce ne soit pas le cas dans la majorité des États Membres.

Contrôle parlementaire

Le contrôle parlementaire est important compte tenu que le parlement contrôle l'activité gouvernementale. Le parlement, en sa qualité de législateur, est chargé d'adopter une législation claire et accessible instituant les services de renseignement et précisant leur organisation, leurs pouvoirs spéciaux et leurs limites. Il est également chargé d'approuver le budget des services de renseignement, et dans certains États membres il s'assure de la conformité de leurs opérations avec le cadre juridique.

- Les conclusions de la FRA indiquent que 24 États membres de l'UE mettent à contribution le parlement ; dans 21 d'entre eux, des commissions parlementaires spécialisées contrôlent les services de renseignement. Plusieurs États membres ont mis en place une commission parlementaire chargée des différents services de sécurité et de renseignement, tandis que d'autres ont créé plusieurs commissions dont chacune est chargée d'un service en particulier.

- Il n'existe dans les États membres de l'UE aucune commission parlementaire qui dispose d'un accès illimité aux informations des services de renseignement.

- Les différentes commissions parlementaires des États membres ont divers mandats : la plupart sont dotées des pouvoirs traditionnels de contrôle liés à la législation, au budget et à la réception d'informations sur le fonctionnement des services, tandis que quelques-unes seulement peuvent traiter des plaintes, rendre des décisions contraignantes sur les services de renseignement ou contribuer à approuver des mesures de surveillance.

- En ce qui concerne le pouvoir des commissions parlementaires d'ouvrir des enquêtes, la législation de la plupart des États membres autorise les commissions à demander des informations aux services de renseignement ou au pouvoir exécutif, mais ne les autorise pas à les exiger.

Contrôle par des experts

Le contrôle par des experts présente un intérêt indéniable car il permet à des individus qui connaissent bien le sujet, qui ont du temps à y consacrer, et qui sont libres de toute influence politique de passer au crible les opérations des services de renseignement. Selon le Commissaire aux droits de l'homme du Conseil de l'Europe, ils sont souvent les mieux placés pour réaliser au jour le jour un contrôle des activités menées par les services de renseignement.

- Bien que le contrôle parlementaire soit déterminant, il doit être complété par d'autres organes de contrôle, en particulier par de solides organismes d'experts qui sont en mesure de superviser les activités opérationnelles, y compris la collecte, l'échange et l'utilisation de données à caractère personnel, ainsi que la protection du droit à la vie privée.

- Dans l'UE, 15 États membres ont mis en place un ou plusieurs organes d'experts spécialisés exclusivement dans le contrôle des services de renseignement. Ils sont compétents notamment pour autoriser des mesures de surveillance, enquêter sur des plaintes, demander des documents et des informations aux services de renseignement, et conseiller le pouvoir exécutif et/ou le parlement. Pour optimiser leur potentiel, il convient de leur accorder l'indépendance, les ressources et les pouvoirs adéquats.

- Dans certains États membres, les institutions qui sont indépendantes des services de renseignement et de l'exécutif ne sont pas impliquées dans l'autorisation des mesures de surveillance.

- Dans les États membres qui sont dotés d'un organe indépendant pour l'autorisation de mesures de surveillance, la surveillance ciblée a tendance à nécessiter une décision de justice, tandis que l'approbation par des organes d'experts est l'alternative privilégiée. Il n'existe pas d'approche commune du contrôle de la collecte de renseignements d'origine technique.

- Il est indispensable que les organes d'experts maîtrisent non seulement les aspects juridiques de la surveillance, mais disposent également de compétences techniques. Certains États membres y veillent en ayant recours à des experts compétents dans divers domaines, y compris les technologies de l'information et de la communication (TIC). D'autres font largement appel à une combinaison de juges et de parlementaires, en poste ou non.

Dans les États membres de l'UE, les autorités chargées de la protection des données (APD), qui sont des organes spécialisés chargés de garantir le respect de la vie privée et la protection des données, jouent un rôle important dans la protection des données à caractère personnel. Ce rôle est consacré par le droit primaire et le droit dérivé de l'UE. Cependant, les organes d'experts spécialisés dans le contrôle des services de renseignement ont incontestablement une expertise reconnue en matière de protection de la vie privée et des données dans le domaine du renseignement.

- Selon les conclusions de la FRA, en comparaison à d'autres activités de traitement des données et à des responsables du traitement des données des secteurs public et privé, les APD de sept États membres ont les mêmes pouvoirs sur les services de renseignement que sur tous les autres responsables du traitement des données. Dans 12 États membres, les APD ne sont pas compétentes pour superviser les services de renseignement, et dans neuf États membres, leurs pouvoirs sont limités.

- Dans les États membres où les APD et d'autres organes d'experts se partagent les compétences, un manque de coopération entre ces derniers est susceptible de créer des lacunes en raison de la fragmentation des responsabilités. Dans les États membres où les APD ne sont pas compétentes pour contrôler les services de renseignement, l'organe de contrôle est chargé de veiller à ce que les garanties qui s'appliquent au respect de la vie privée et à la protection des données soient bien appliquées.

- Les recherches menées précédemment par la FRA sur l'accès aux voies de recours en matière de protection des données soulignent la nécessité d'améliorer la capacité des APD ; il s'agit d'un point important compte tenu du rôle que les APD pourraient jouer dans la supervision des services de renseignement.

Voies de recours

Selon les normes internationales applicables, toute personne qui s'estime être victime d'une violation de la protection de la vie privée ou du droit à la protection des données doit avoir la possibilité d'engager un recours. Le droit à un recours effectif – qui permet aux personnes de demander réparation en cas de violation de leurs droits – est un élément essentiel de l'accès à la justice. Un recours doit être « effectif » en pratique et en droit.

Comme le montrent de précédents rapports de la FRA sur l'accès aux voies de recours et à la justice dans le domaine de la protection des données, les victimes de violations de la protection de la vie privée et des données à caractère personnel ont à leur disposition plusieurs voies de recours. Les organes extra-juridictionnels jouent un rôle important parmi les différentes voies de recours dans le domaine de la surveillance, compte tenu des difficultés pratiques pour saisir les tribunaux. Les organes extra-juridictionnels dans les 28 États membres de l'UE comprennent des organes d'experts (dont des APD), des organes exécutifs et parlementaires, ainsi que les médiateurs. Dans plusieurs États membres, le nombre d'organes extra-juridictionnels jouant un rôle dans des recours relevant du domaine de la surveillance est relativement satisfaisant, mais il devrait être examiné en tenant compte des observations qui suivent.

La complexité du paysage de recours ne facilite pas la mise en œuvre de recours effectifs, pas plus que le volume de données collectées par les services de renseignement qui appliquent le SIGINT. Il est difficile de former un recours en raison de la fragmentation et du cloisonnement des différentes voies de recours. En réalité, les données collectées montrent que seul un petit nombre d'affaires mettant en cause les pratiques de surveillance ont été jugées au niveau national depuis les révélations d'Edward Snowden.

Obligation d'informer et droit d'accès

Le droit d'être informé et d'accéder à l'information est essentiel pour que des personnes sous surveillance puissent engager des recours. La Cour européenne des droits de l'homme (CouEDH) a toutefois accepté que ces droits puissent être limités pour des motifs justifiés (voir CouEDH, *Klass et autres c. Allemagne,* n° 5029/71, 6 septembre 1978). Les conclusions de la FRA indiquent que le secret entourant le travail des services de renseignement limite effectivement ces droits. Il convient de tenir compte d'un autre facteur qui est le volume considérable de données collectées par le SIGINT en comparaison à d'autres formes de surveillance plus traditionnelles.

- Dans huit États membres, la loi ne prévoit en aucun cas l'obligation d'informer et le droit d'accès ; des règles sur les documents qui font l'objet d'un classement ou sur des secrets d'État sont applicables. Dans les 20 autres États membres, la législation prévoit l'obligation d'informer et le droit d'accès, parfois dans des délais bien précis, mais avec certaines restrictions. Ces restrictions sont fondées sur plusieurs motifs, tels que la sécurité nationale, les intérêts nationaux ou la finalité de la mesure de surveillance en question.

- Deux États membres seulement ont des dispositions spécifiques sur l'obligation d'informer dans le contexte du renseignement d'origine électromagnétique : dans le premier, les personnes ne sont pas informées si les sélecteurs utilisés ne lui sont pas directement imputables à l'individu ; dans l'autre, la personne ne l'est pas si les données à caractère personnel obtenues sont immédiatement effacées après la collecte et si elles ne sont pas traitées ultérieurement.

- Les organes de contrôle de 10 États membres de l'UE, dont 6 APD, contrôlent les restrictions relatives au droit d'être informé et au droit d'accès à l'information en vérifiant si la menace invoquée pour la sécurité nationale est raisonnable, et/ou en exerçant indirectement le droit d'accès de la personne concernée. Dans ce dernier cas, les organes déterminent si l'accès aux données peut être accordé ou si le refus de l'accorder est légitime, et ils examinent également la licéité du traitement de données. Dans un État membre, une décision juridictionnelle – attestant que la notification compromettrait l'enquête ou qu'il existe d'autres arguments qui s'y opposent – est requise.

- Deux autres États membres ne prévoient pas de droit d'accès à l'information en tant que tel. La loi prévoit néanmoins un droit qui conduit au même résultat : une personne peut demander à l'organe de contrôle de vérifier si ses données font l'objet d'une surveillance illégale.

- Dans certains États membres, l'organe de contrôle qui contribue indirectement à l'exercice du droit d'une personne de demander l'accès aux données ne confirme pas le traitement des données pas plus qu'il ne le rejette. Les réponses se limitent généralement à indiquer que la plainte a été traitée et/ou vérifiée.

Recours juridictionnels

Chaque État membre donne aux personnes la possibilité de saisir les tribunaux pour se plaindre d'atteintes à la vie privée, qu'elles résultent d'une surveillance ciblée ou de renseignements d'origine électromagnétique. Les tribunaux représentent une voie de recours pour les personnes souhaitant se plaindre d'une ingérence dans leur vie privée, y compris celles souhaitant contester des décisions d'organes de contrôle concernant leur action pour atteinte à la vie privée. Ils donnent aussi aux personnes la possibilité de demander réparation – y compris dans le domaine de la surveillance.

- Cependant, les précédentes recherches de la FRA ont mis en évidence l'absence de spécialisation des juges dans le domaine de la protection des données, ce qui représente un obstacle important à une réparation effective des atteintes à la protection des données. Cette conclusion s'applique aussi au domaine de la surveillance, dans lequel, outre le secret nécessaire lié au renseignement, une expertise pertinente dans le domaine des TIC ou des renseignements, par exemple, est essentielle.

- Seulement deux États membres ont limité l'absence de spécialisation dans le contexte de recours en faisant appel à des juges ou tribunaux qui disposent à la fois des connaissances nécessaires pour se prononcer (souvent) sur des questions techniques, et qui sont autorisés à accéder aux documents secrets.

Recours extra-juridictionnels

Les mécanismes extra-juridictionnels sont généralement plus accessibles car les règles de procédure sont moins strictes et la procédure de recours est plus rapide et moins coûteuse. Des données précédemment publiées par la FRA le confirment, en particulier dans le contexte de la protection des données, puisque les APD sont saisies d'un plus grand nombre de plaintes et seuls quelques plaignants engagent des poursuites en justice. Les organes extra-juridictionnels – autres que les APD – qui œuvreraient dans le domaine de la protection des données sont cependant peu nombreux et un grand nombre d'organes extra-juridictionnels n'ont qu'un pouvoir limité lorsqu'il s'agit d'offrir un recours.

- Les organes de contrôle (y compris les APD) qui sont chargés d'examiner les plaintes sont des institutions indépendantes dans la grande majorité des États membres.

- Lorsqu'un organe de contrôle exécutif a le pouvoir d'offrir un recours, la question de l'indépendance se pose lorsqu'il a aussi le pouvoir de garantir la surveillance. Les organes de contrôle parlementaire et les organes d'experts sont dotés de structures administratives plus autonomes – mais l'autonomie ne garantit pas un recours effectif, sauf si elle s'accompagne aussi de connaissances suffisantes. Lorsqu'il s'agit d'évaluer le degré d'indépendance d'un organe, il est aussi important de tenir compte de la façon dont les membres des organes de contrôle sont nommés et de la place qu'ils occupent dans la hiérarchie administrative.

- Les APD de 13 États membres de l'UE sont dotées du pouvoir d'examiner des plaintes individuelles et de rendre des décisions contraignantes. Mais pour trois d'entre elles, le pouvoir d'accéder à des dossiers et des locaux est limité. Dans cinq États membres, des dispositions supplémentaires – exigeant la présence du directeur ou d'un membre de l'APD lors des inspections dans les locaux des services de renseignement – s'appliquent.

- Sur les sept États membres qui confèrent à leurs organes d'experts (autres que les APD) les pouvoirs spécifiques d'offrir un recours, cinq les autorisent à prendre des décisions contraignantes. Dans deux État membres de l'UE, un organe de contrôle exécutif dispose aussi de ces pouvoirs. Les commissions parlementaires de quatre États membres sont habilitées à recevoir des plaintes individuelles, mais une seule peut les régler par des décisions contraignantes.

- Les médiateurs, qui existent dans les 28 États membres de l'UE, traitent essentiellement de défaillances administratives plutôt que du bien-fondé de la surveillance. Seul un État membre confère à l'institution du médiateur le pouvoir d'offrir un recours en vertu de la loi correspondante sur le renseignement. En outre, les pouvoirs des institutions des médiateurs peuvent être assez limités, et la procédure aboutit généralement à des recommandations non contraignantes qui visent à remédier à la situation et orienter les mesures futures, plutôt qu'à une décision contraignante et exécutoire. Cela a manifestement une incidence sur l'effectivité des recours qu'ils sont en mesure d'offrir.

- D'autres éléments susceptibles de faciliter l'accès d'une personne aux voies de recours comprennent des règles plus souples sur la charge de la preuve et les actions collectives, ainsi qu'une protection efficace des lanceurs d'alerte. L'Assemblée parlementaire du Conseil de l'Europe estime que le fait de donner l'alerte est le moyen le plus efficace pour assurer le respect des limites imposées aux opérations de surveillance.

Conclusions

Dans un domaine où la compétence de l'UE est restreinte, le rapport souligne la diversité qui existe parmi les États membres en ce qui concerne la manière dont les services de renseignement sont organisés et dont ils s'acquittent de leur mission principale.

Les mesures de surveillance constituent une ingérence considérable dans les droits des personnes. Compte tenu de leur caractère secret, les personnes sont tenues de faire confiance aux pouvoirs publics qui, à leur tour, se doivent de protéger les droits fondamentaux de ces personnes. Pour atteindre le niveau de confiance qu'une société doit avoir vis-à-vis de ses services de renseignement, l'obligation de rendre compte est primordiale. Une législation claire et accessible, des mécanismes de supervision solides, des mécanismes de contrôle appropriés et des recours effectifs ne sont que quelques-uns des éléments essentiels pour parvenir à ce type de responsabilisation, qui reste indéniablement difficile en raison du secret qui entoure les opérations des services de renseignement. Le fait d'introduire et de maintenir une législation claire et accessible et des mécanismes de contrôle solides au niveau des États membres n'est que la première étape vers un système respectueux des droits fondamentaux – toute difficulté pour y parvenir suggère que des obstacles existent toujours.

Les réactions suscitées par les révélations d'Edward Snowden ont souligné la nécessité d'adapter et de renforcer les cadres juridiques correspondants dans l'UE et ses États membres. Les recherches de la FRA indiquent qu'un certain nombre de réformes juridiques ont déjà été engagées. Des évaluations régulières du fonctionnement et de la légitimité des cadres qui régissent l'activité des services de renseignement doivent devenir partie intégrante des systèmes de contrôle. Une question clé est de savoir comment réformer davantage les cadres juridiques pour tenir compte du manque de contrôle approprié. En outre, les réformes engagées dans les États membres de l'UE doivent tenir compte des récentes évolutions technologiques pour faire en sorte que les mécanismes de contrôle disposent des outils et de l'expertise requis. Tous ces objectifs sont incontestablement ambitieux, mais essentiels pour s'acquitter de la mission difficile qui consiste à protéger la sécurité tout en garantissant les les droits fondamentaux.

Protéger la population des menaces à la sécurité et garantir les droits fondamentaux implique un équilibre fragile. Les attaques terroristes brutales et les innovations technologiques qui rendent possibles des communications et le contrôle de données à grande échelle ont compliqué davantage la situation et ont suscité des préoccupations quant aux violations des droits à la vie privée et à la protection des données commises au nom de la protection de la sécurité nationale. Les révélations d'Edward Snowden, qui ont mis au jour de vastes opérations de surveillance indiscriminée à travers le monde, ont souligné la nécessité de renforcer la protection de ces droits.

Le rapport, rédigé en réponse à la demande du Parlement européen d'effectuer des recherches approfondies sur la protection des droits fondamentaux dans le contexte de la surveillance, établit un panorama et analyse les cadres juridiques en place dans les États membres de l'UE en matière de surveillance. Axé sur ce qu'il convient d'appeler la « surveillance de masse », il présente aussi en détail les mécanismes de contrôle mis en place à travers l'UE, décrit les travaux des entités chargées de contrôler les opérations de surveillance, et présente les voies de recours mises à disposition des personnes qui souhaitent contester les activités de renseignement qui les visent. En mettant en évidence les considérations complexes qui sont en jeu, le présent rapport souligne en quoi il peut être difficile de tenir compte de ce qui est souvent considéré comme des priorités concurrentes, et contribue au débat permanent sur la manière de les concilier au mieux.

Informations supplémentaires :

Pour consulter le rapport intégral de la FRA *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'UE - Panorama du droit des États membres) voir : http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

Nous vous invitons à consulter les publications suivantes :

- FRA et Conseil de l'Europe (2014), *Manuel de droit européen en matière de protection des données*, Luxembourg, Office des publications, http://fra.europa.eu/fr/publication/2014/manuel-de-droit-europen-en-matire-de-protection-des-donnes (disponible dans les langues de l'UE)
- FRA (2014), *Access to data protection remedies in EU Member States*, Luxembourg, Office des publications, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states et *Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE - Résumé* http://fra.europa.eu/fr/publication/2014/accs-aux-voies-de-recours-en-matire-de-protection-des-donnes-caractre-personnel (disponible dans les langues de l'UE)

Un aperçu des activités de la FRA consacrées à la protection des données est disponible à l'adresse suivante : http://fra.europa.eu/fr/theme/protection-des-donnees-et-vie-privee.

Office des publications

FRA – AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE

Schwarzenbergplatz 11 – 1040 Vienne – Autriche
Tél. : +43 158030-0 – Fax : +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Print: ISBN 978-92-9491-025-7, doi:10.2811/482778
PDF: ISBN 978-92-9491-052-3, doi:10.2811/77109

TK-04-15-738-FR-C (print); TK-04-15-738-FR-N (PDF)