Strasbourg, le 13 décembre 2024 **CDL-AD(2024)043**

Or. angl.

COMMISSION EUROPEENNE POUR LA DEMOCRATIE PAR LE DROIT

(COMMISSION DE VENISE)

RAPPORT

SUR

UNE REGLEMENTATION DES LOGICIELS ESPIONS CONFORME A L'ETAT DE DROIT ET AUX DROITS HUMAINS

Adopté par la Commission de Venise
à sa 141e session plénière
(Venise, 6-7 décembre 2024)

Sur la base des commentaires de :

M. Iain CAMERON (membre, Suède)
M. David A. KAYE (membre, Etats-Unis d'Amérique)
M. Tuomas OJANEN (membre, Finlande)
M. Timothy OTTY (membre, Royaume-Uni)
Mme Tamar KALDANI (experte, Géorgie)

Table des matières

I. Introduction

1. Par lettre du 6 décembre 2023, le président de l'Assemblée parlementaire du Conseil de l'Europe (APCE) de l'époque, M. Tiny Kox, a demandé à la Commission de Venise, conformément à la Résolution 2513 (2023) de l'APCE sur « Le logiciel espion Pegasus et les autres types de logiciels similaires, et la surveillance secrète opérée par l'État »[1], de mener une étude sur le cadre législatif et la pratique en matière de surveillance ciblée de tous les États membres du Conseil de l'Europe (en priorité la Pologne, la Hongrie, la Grèce, l'Espagne et l'Azerbaïdjan ; puis l'Allemagne, la Belgique, le Luxembourg, les Pays-Bas et l'ensemble des autres États membres).

2. Dans sa Résolution 2513(2023), l'APCE avait demandé à certains Etats membres de l'informer, ainsi que la Commission de Venise, de l'utilisation de Pegasus et d'autres logiciels espions similaires[2] ou de clarifier le cadre juridique de leur utilisation et les mécanismes de contrôle applicables[3]. En particulier, l'APCE a demandé à la Commission de Venise d'évaluer le cadre législatif et la pratique en matière de surveillance ciblée de tous les Etats membres (en priorité ceux concernés par la Résolution), afin de déterminer si ces cadres contiennent des garanties adéquates et efficaces contre tout abus éventuel de logiciels espions, eu égard à la Convention et à d'autres normes du Conseil de l'Europe[4].

3. MM. Iain Cameron, David A. Kaye, Tuomas Ojanen et Timothy Otty ont été les rapporteurs de ce rapport. Mme Tamar Kaldani, ancienne première vice-présidente et membre élue du comité consultatif de la Convention 108 du Conseil de l'Europe, a été invitée à rejoindre le groupe de travail en tant qu'experte.

4. En réponse à cette demande, la Commission de Venise a mené une étude comparative pour évaluer les règles existantes en matière de surveillance ciblée et notamment d'utilisation de logiciels espions dans ses Etats membres. La Commission de Venise a examiné les dispositions juridiques des Etats qui ont envoyé des informations officielles à l'APCE[5] et de ceux sur lesquels les membres de la Commission de Venise/experts ont fourni des informations en répondant à un questionnaire préparé par les rapporteurs (CDL-PI(2024)014)[6]. D'autres informations ont été recueillies par le biais de recherches documentaires[7]. Le matériel recueilli est disponible par pays et par question.

---

[1] APCE, Résolution 2513(2023), *Le logiciel espion Pegasus et les autres types de logiciels similaires, et la surveillance secrète opérée par l'État*, 11 octobre 2023. Comme expliqué dans la résolution et détaillé ci-dessous, Pegasus est un logiciel espion développé par une société israélienne, NSO, et est peut-être aujourd'hui le plus connu des différents logiciels espions utilisés par les États ces dernières années.
[2] Pologne, Hongrie, Grèce, Espagne et Azerbaïdjan, § 11 de la résolution.
[3] Allemagne, Belgique, Luxembourg et Pays-Bas, § 13 de la résolution.
[4] § 15 de la résolution.
[5] L'APCE a partagé avec la Commission de Venise les réponses qu'elle a reçues, à savoir de l'Azerbaïdjan, de l'Allemagne, de la Grèce, du Luxembourg, des Pays-Bas, de la Pologne et de l'Espagne. La Belgique et la Hongrie n'ont pas envoyé de réponses.
[6] Des réponses à ce questionnaire et à une demande d'information plus générale, envoyée en février 2024, dans laquelle les rapporteurs s'enquéraient du cadre juridique régissant l'utilisation de Pegasus et d'autres logiciels espions équivalents, ont été reçues de l'Autriche, de la Belgique, de la Bulgarie, de la Bosnie-Herzégovine, du Canada, de la Croatie, de Chypre, du Danemark, de l'Estonie, de la Finlande, de la France, Allemagne, Grèce, Islande, Irlande, Italie, Kosovo, Kirghizstan, Liechtenstein, Lituanie, Malte, République de Moldova, Monaco, Maroc, Pays-Bas, Macédoine du Nord, Norvège, Pologne, Portugal, Roumanie, Saint-Marin, Serbie, République slovaque, Corée du Sud, Espagne, Suède, Suisse, Türkiye, Ukraine, Royaume-Uni, États-Unis d'Amérique..
[7] *Voir notamment* Parlement européen, *Utilisation de Pegasus et de logiciels espions de surveillance équivalents Cadre juridique des États membres en matière d'acquisition et d'utilisation de Pegasus et de logiciels espions de surveillance équivalents* (« Étude PEGA »), 5 décembre 2022 et le rapport de l'Agence des droits fondamentaux, *Surveillance by intelligence services : Fundamental rights safeguards and remedies in the EU - 2023 update* (« Rapport FRA »), 24 mai 2023. Le rapport de la FRA constitue une mise à jour partielle des rapports de la FRA de 2015 et 2017.

5. Ce rapport a été rédigé sur la base des commentaires des rapporteurs et des résultats de la recherche comparative. Il a été adopté par la Commission de Venise lors de sa 141e session plénière (Venise, 6-7 décembre 2024).

II. Contexte et portée du rapport

6. Il existe plusieurs termes qui font référence au type de surveillance ciblée en question : « logiciel espion », « logiciel de surveillance intrusif », ou le terme plus neutre d'« exploitation des réseaux informatiques ». Dans le présent rapport, la Commission de Venise utilisera le terme « logiciel espion » qui est également utilisé dans la demande de l'APCE.

7. Le terme « logiciel espion » est un terme générique qui englobe les logiciels de surveillance intrusifs pouvant être utilisés pour interférer avec des appareils électroniques, notamment des smartphones ou des ordinateurs, à l'insu de l'utilisateur, et qui permettent à l'opérateur de pénétrer dans l'appareil et, selon l'outil spécifique, de suivre la géolocalisation en temps réel, de lire toutes les données stockées et toutes les communications effectuées (en contournant les protections éventuelles, telles que le cryptage), et de prendre le contrôle de tous les matériels et logiciels disponibles sur l'appareil, y compris les microphones ou les caméras[8]. Contrairement aux écoutes téléphoniques classiques, les logiciels espions peuvent potentiellement fournir un accès complet et rétroactif aux fichiers et aux messages créés dans le passé, aux mots de passe et aux métadonnées relatives aux communications antérieures. L'article 2, paragraphe 20, du Règlement (CE) n° 2024/1083 (législation européenne sur la liberté des médias) définit le « logiciel de surveillance intrusif »[9] comme « *tout produit comportant des éléments numériques spécialement conçus pour exploiter les vulnérabilités d'autres produits comportant des éléments numériques, qui permet la surveillance secrète de personnes physiques ou morales par le contrôle, l'extraction, la collecte ou l'analyse de données provenant de ces produits ou des personnes physiques ou morales qui utilisent ces produits, y compris de* manière *indiscriminée* »[10].

8. Les logiciels espions peuvent infecter les appareils ciblés par le biais de divers mécanismes : ils peuvent être implantés par un accès physique à un appareil, mais aussi par l'implantation à distance d'un « cheval de Troie », d'un virus ou d'un programme. Il peut s'agir d'envoyer un message (SMS, courrier électronique ou applications de messagerie en ligne) contenant un lien vers un site web qui, s'il est visité, infectera l'appareil. Certains outils utilisent l'attaque dite « zéro-clic », dans laquelle la simple réception d'un message entraîne l'infection du logiciel espion, sans qu'aucune interaction de la part de l'utilisateur ne soit nécessaire. La détection des infections par logiciels espions nécessite des compétences techniques de haut niveau et leur présence sur un appareil peut être difficile à prouver[11]. Les logiciels espions les plus intrusifs, tels que Pegasus, peuvent secrètement transformer un téléphone portable ou un ordinateur personnel en un dispositif de surveillance 24 heures sur 24, permettant à un opérateur d'avoir un accès complet à tous les capteurs et à toutes les informations de l'appareil personnel.

9. L'utilisation abusive de logiciels espions commerciaux a donné lieu à de très graves violations des droits humains. Une coalition internationale de journalistes d'investigation a rapporté que plus de 50 000 personnes, dont des défenseurs des droits humains, des opposants politiques, des avocats, des diplomates, des chefs d'État et près de 200 journalistes de 24 pays, avaient été

[8] Le terme « logiciel espion » en tant que tel n'est pas utilisé dans la législation que la Commission de Venise a évaluée. Voir également le paragraphe 40 ci-dessous.
[9] Le considérant 25 de la législation européenne sur la liberté des médias (voir ci-dessous) inclut les « logiciels espions » dans la définition des « logiciels de surveillance intrusifs ».
[10] Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias). La législation européenne sur la liberté des médias est entrée en vigueur le 7 mai 2024 et s'appliquera pleinement à partir du 8 août 2025.
[11] *Ibidem*, p. 7 et suivantes.

identifiées comme des cibles potentielles de logiciels espions d'État[12]. Le rapport de l'APCE constate qu'il y a de plus en plus de preuves que Pegasus et des logiciels espions similaires ont été utilisés illégalement ou à des fins illégitimes par plusieurs États membres, notamment contre des journalistes, des opposants politiques, des défenseurs des droits humains et des avocats[13]. L'APCE a également relevé des preuves que des États membres du Conseil de l'Europe ont exporté des systèmes de surveillance intrusifs présentant des caractéristiques similaires à Pegasus vers des pays tiers dotés de régimes autoritaires et présentant un risque élevé de violations des droits humains.

10. Plusieurs logiciels espions différents ont été développés, utilisés et exportés par ou pour des États dans le monde entier. L'expansion considérable des communications numériques a poussé les États à trouver des outils pour permettre la surveillance dans le cadre de l'application de la loi et du renseignement. En ce qui concerne les réseaux nationaux de télécommunications, les États ont imposé aux fournisseurs de télécommunications l'obligation de permettre aux services de police et de renseignement d'accéder aux communications sous une forme accessible, en contournant le cryptage qui est devenu la norme pour les fournisseurs de télécommunications et les fabricants d'appareils. Dans certaines juridictions, en particulier lorsque le suspect sait qu'il fait l'objet d'une enquête, il est possible qu'un tribunal ordonne au fabricant ou au fournisseur d'« ouvrir » l'appareil. Toutefois, les services de police et de renseignement ont fait valoir que lorsqu'un tribunal n'est pas en mesure d'exécuter une telle ordonnance à l'encontre du fabricant ou du fournisseur, et qu'il n'est donc pas possible d'obtenir un accès ordonné par le tribunal, il est nécessaire d'obtenir un accès d'une manière ou d'une autre aux appareils de communication eux-mêmes (ordinateurs portables, téléphones mobiles, etc.).

11. Les États affirment en outre la nécessité d'utiliser des logiciels espions pour défendre leur sécurité nationale et publique contre les menaces, y compris la criminalité, et contre les activités visant à déstabiliser leurs structures constitutionnelles, politiques, économiques ou sociales fondamentales. Les développements technologiques limitent la capacité des autorités chargées de l'application de la loi à accéder aux données par les méthodes précédemment établies. Par conséquent, certains États affirment que la surveillance intrusive de l'appareil d'un suspect est nécessaire pour mener à bien leurs enquêtes, en particulier pour accéder à des données autrement protégées par le cryptage[14].

12. Toutefois, comme il ressort de la description préliminaire des capacités des logiciels espions présentée ci-dessus, le risque de surveillance intrusive injustifiée ou disproportionnée à l'aide d'un tel outil est important. S'ils ne sont pas réglementés, les logiciels espions constituent une arme de surveillance puissante qui peut être utilisée pour restreindre les droits humains, censurer et criminaliser la critique et la dissidence, harceler (voire supprimer) les journalistes, les défenseurs des droits humains, les opposants politiques et réprimer les organisations de la

[12] Forbidden stories, *The Pegasus project : a worldwide collaboration to counter a global crime*, 18 juillet 2021.
[13] Assemblée parlementaire du Conseil de l'Europe, Rapport n° 15825, *Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État* (« Rapport de l'APCE »), 20 septembre 2023, Exposé des motifs §§ 6-63.
[14] Comme l'a constaté le Comité permanent belge de contrôle des services de renseignement et de sécurité : « *[S]ans nier toute l'importance que conservent des méthodes et techniques plus classiques de renseignement comme la collecte et l'analyse d'origine humaine ou « HUMINT » (Human Intelligence), il est incontestable que le recours à des outils technologiques de renseignement et de sécurité comme les Remote Infection Technologies est de nature à renforcer significativement la position d'information des services. En outre, force est de constater que la baisse de l'effectivité des mesures d'interception plus classiques des communications est démontrée par la complexification de la collecte et du traitement des informations. Cette situation contrarie de plus en plus, voire empêche, le cycle de renseignement et ses objectifs d'anticiper les risques de sécurité et de permettre un conseil adéquat aux autorités sur la manière de traiter les menaces, voire de les entraver directement* » ; *voir* Comité permanent de contrôle des services de renseignement et de sécurité, *Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel PEGASUS*, 17 octobre 2022. Voir également Chambre des communes, Canada, *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés - Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, novembre 2022, section sur les avantages des outils d'enquête technologiques, p. 8-9.

société civile. Des rapports d'expertise substantiels établis par des organisations de la société civile - notamment par Citizen Lab[15], Amnesty Tech[16] et AccessNow[17] - ont permis d'identifier des preuves significatives de surveillance abusive à l'aide de logiciels espions.

13. L'utilisation de logiciels espions par les forces de l'ordre ou les services de renseignement constitue un cas de « surveillance ciblée » puisqu'elle se concentre sur des individus ou des groupes identifiés. Dans le présent rapport, on entend par « surveillance ciblée » la surveillance délibérée d'individus ou de groupes spécifiques par les services de police ou de renseignement[18].

14. Traditionnellement, la surveillance ciblée exige beaucoup de ressources. Cela semble toujours être le cas pour l'utilisation de logiciels espions. Les logiciels espions exploitent les failles de sécurité des appareils ou des applications particulières, qui sont ensuite utilisées pour donner au « pirate » le contrôle de l'appareil en tant que tel[19]. En raison de l'expertise technique importante requise, certains gouvernements achètent des services de logiciels espions à un opérateur commercial, ce qui peut s'avérer coûteux[20]. Cela dit, comme le note la Commission de Venise dans sa liste de contrôle sur l'État de droit, les développements techniques rendent la surveillance « de plus en plus facile à utiliser »[21]. Cela signifie que la technologie de surveillance devient accessible à une série d'États qui peuvent manquer d'expertise technique nationale et de garanties systématiques en matière de droits humains. Il est donc essentiel que les garanties strictes qui défendent les droits humains et l'État de droit soient appliquées au développement et à l'utilisation de technologies telles que les logiciels espions, afin d'éviter de donner aux États le pouvoir d'interférer avec les protections et les garanties qui sont nécessaires dans une société démocratique.

15. Sur la base des résultats de l'étude comparative des cadres juridiques régissant l'utilisation des logiciels espions dans ses Etats membres et en s'appuyant sur la jurisprudence de la Cour européenne des droits de l'homme (CourEDH) en matière de surveillance ciblée, la Commission de Venise a tenté d'identifier les garanties minimales qui devraient être mises en place, lorsqu'il s'agit de mesures intrusives de surveillance ciblée, afin de prévenir les pratiques de surveillance illégales. La complexité des cadres législatifs en question, le manque d'informations complètes et pratiques sur la mise en œuvre des normes internationales existantes, telles que l'article 9 de

---

[15] *Voir, par exemple*, Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuous Proliferation*, 15 octobre 2015; "*The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*", 24 août 2016; "*HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 18 septembre 2018; *Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, 16 décembre 2021; "*GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement*, 17 juillet 2022; "*PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions*", 22 septembre 2023.

[16] *Voir, par exemple*, Amnesty Tech, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, 18 juillet 2021; *Dominican Republic: Pegasus spyware discovered on prominent journalist's phone*, 2 mai 2023; *Global: A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia*, 2 mai 2024.

[17] *Voir, par exemple,* Access Now, *Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict*, 25 May 2023; *Hacking Meduza: Pegasus spyware used to target Putin's critic*, 13 septembre 2023; *New spyware attacks exposed: civil society targeted in Jordan*, 1 février 2024; *Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware*, 30 mai 2024.

[18] Par opposition à la surveillance stratégique ou « en vrac », qui consiste plutôt en la collecte généralisée de très grandes quantités de données de contenu électronique et de métadonnées, qui sont ensuite soumises à une analyse informatique à l'aide de sélecteurs.

[19] Les applications sont normalement conçues de manière à être « étanches » les unes par rapport aux autres. Même si une vulnérabilité peut être trouvée, il se peut qu'elle ne puisse pas être exploitée suffisamment. Des « attaques » répétées peuvent s'avérer nécessaires, et même dans ce cas, elles peuvent ne pas être couronnées de succès. Il y a souvent une part considérable de hasard dans l'efficacité ou l'inefficacité du logiciel espion. Le processus d'exécution à distance d'un logiciel espion étant très technique et prenant généralement beaucoup de temps, il nécessite une équipe de spécialistes.

[20] En 2016, il a été rapporté que le NSO a facturé aux agences gouvernementales 650 000 dollars pour l'utilisation de Pegasus sur dix cibles, plus 500 000 dollars de frais d'installation

[21] Commission de Venise, CDL-AD(2016)007, *Liste des critères de l'Etat de droit*, § 118.

la Convention 108, ainsi que la rareté des réglementations spécifiques aux logiciels espions ont été des facteurs importants à prendre en compte lors de la préparation du rapport. Les exemples cités dans le rapport ne sont pas exhaustifs et ne sont présentés qu'à des fins de comparaison. Le fait qu'ils soient mentionnés ne signifie pas que la Commission de Venise les approuve tacitement comme étant compatibles avec les droits humains et l'Etat de droit. En fin de compte, il appartiendra à la CourEDH, dans le cadre de l'examen des affaires liées aux « logiciels espions »[22], de fixer les normes minimales applicables dans ce domaine. Une contribution importante à la définition de ces normes au niveau mondial peut également être apportée par le Comité de la Convention 108+ dans le cadre de ses travaux sur l'interprétation de l'article 11 et du mécanisme d'évaluation et de suivi à mettre en œuvre au titre de la Convention 108+.

III. La jurisprudence de la CourEDH et d'autres normes européennes et internationales concernant les logiciels espions[23]

A. La jurisprudence de la CourEDH sur le droit au respect de la vie privée et les travaux antérieurs de la Commission de Venise

16. Il n'est pas contesté que les données personnelles contenues dans un appareil, y compris les communications mobiles/téléphoniques, sont couvertes par les notions de « vie privée » et de « correspondance ». L'utilisation de logiciels espions interfère directement avec le droit au respect de la vie privée consacré par l'article 8 de la Convention européenne des droits de l'homme (CEDH) et l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP). Une telle ingérence ne peut être autorisée qu'à trois conditions : les conditions dans lesquelles l'ingérence peut se produire doivent être définies clairement par la loi, dans une législation ou une réglementation qui doit être accessible à l'individu concerné et le protéger contre l'arbitraire, notamment par sa précision et sa prévisibilité ; elle doit servir l'un des buts légitimes énumérés à l'article 8, paragraphe 2, de la CEDH ;[24] et elle doit correspondre à un besoin social impérieux[25] et être proportionnée au but légitime poursuivi, de sorte qu'elle puisse être considérée comme nécessaire dans une société démocratique. Les trois conditions énumérées ci-dessus sont cumulatives et chacune a une fonction autonome à remplir. Les ingérences disproportionnées dans le droit au respect de la vie privée ne sont pas compatibles avec la Convention, même dans le but d'atteindre des objectifs légitimes et très urgents.

17. Selon les circonstances de chaque cas, l'utilisation de logiciels espions peut également porter atteinte à plusieurs autres libertés et droits humains (par exemple, le droit à un procès équitable, la liberté de religion, la liberté d'expression, la liberté de réunion et d'association, la liberté de circulation, le droit à des élections libres, le droit à la non-discrimination[26], le droit de ne pas être

---

[22] Voir CourEDH *Brejza c. Pologne et 8 autres* (communication), no 27830/23 et 8 autres, 3 juillet 2024 ; voir aussi *Koukakis c. Grèce* (communication), no. 37659/22, 10 janvier 2024 ; pour un historique factuel de l'affaire, *voir Rapport d'enquête sur des allégations d'infractions et de mauvaise administration dans l'application du droit de l'Union en relation avec l'utilisation de Pegasus et de logiciels espions de surveillance équivalents* (2022/2077(INI)) (« Rapport PEGA »), 22 mai 2023, §§ 202-210 et le rapport de l'APCE, cité ci-dessus, exposé des motifs §§ 31-35. L'affaire a finalement été déclarée irrecevable par la CourEDH en raison d'un abus du droit de recours, *voir* CourEDH, *Koukakis c. Grèce* (décision), no. 37659/22, 11 juin 2024.

[23] Un aperçu détaillé des normes internationales et du Conseil de l'Europe existantes et applicables figure dans le rapport de l'APCE, cité ci-dessus, exposé des motifs, §§ 64-80.

[24] Ou, dans le cadre du PIDCP, se conformer aux dispositions, buts et objectifs du Pacte, voir Haut-Commissariat des Nations unies aux droits de l'homme, *Observation générale no 16: Article 17 (Droit au respect de la vie privée)*, 8 avril 1988, §§ 3-4.

[25] CourEDH, *Dudgeon c. Royaume-Uni*, n° 7525/76, 22 octobre 1981, § 51.

[26] Des problèmes peuvent en effet se poser lorsque la surveillance est basée sur des algorithmes ou sur d'autres méthodes permettant de « profiler » des individus en vue d'une surveillance ciblée en raison de leur appartenance à un groupe racial, ethnique, culturel, religieux, politique ou autre. Le profilage non discriminatoire dans un contexte de droit pénal est, en principe, un moyen admissible d'activité des services répressifs : des profils détaillés basés sur des facteurs dont la corrélation avec certains comportements criminels est statistiquement prouvée peuvent être des outils efficaces pour mieux cibler les ressources limitées des services répressifs. Toutefois, une différence

soumis à des traitements inhumains ou dégradants[27]), soit directement, soit par le biais d'un « effet de refroidissement » résultant d'une intrusion de premier ordre dans les droits à la vie privée qui a également une incidence sur la jouissance ou l'exercice par les individus de leurs autres droits[28]. En outre, les logiciels espions peuvent affecter non seulement les droits humains des cibles directes, mais aussi ceux des autres personnes, y compris les enfants, qui sont en contact avec elles. Étant donné que le droit à la protection de la vie privée (et le droit à la protection des données à caractère personnel, qui est reconnu comme un attribut important du droit à la vie privée dans la jurisprudence de la CourEDH) tend à être le droit fondamental le plus souvent et le plus directement affecté par l'utilisation de logiciels espions, le présent rapport se concentre sur les interférences avec l'article 8 de la CEDH.

18. La CourEDH doit encore développer une jurisprudence spécifique sur la proportionnalité de l'utilisation des logiciels espions. Cependant, elle a déjà produit une jurisprudence substantielle dans le domaine de la surveillance en général, où elle a établi une distinction entre la surveillance ciblée et l'interception en vrac[29]. Dans l'*affaire Roman Zakharov c. Russie,* la Grande Chambre de la Cour a codifié les garanties minimales suivantes qui devraient être inscrites dans la loi, lorsqu'il s'agit de mesures de surveillance ciblée (secrète), afin d'éviter les abus de pouvoir : (i) une déclaration claire de la nature des infractions pouvant donner lieu à une ordonnance d'interception ; (ii) une définition des catégories de personnes susceptibles d'être mises sur écoute ; (iii) une limite à la durée de l'interception ; (iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données obtenues ; (v) les précautions à prendre lors de la communication des données à d'autres parties ; et (vi) les circonstances dans lesquelles les enregistrements peuvent ou doivent être effacés ou détruits[30]. Dans le même arrêt, la CourEDH a également établi une obligation générale de notification rétrospective, sous réserve

---

de traitement fondée sur un critère tel que la race, l'appartenance ethnique, l'origine nationale ou la religion ne sera compatible avec le principe de non-discrimination que si elle est étayée par des motifs objectifs et raisonnables. Ainsi, la différence de traitement doit poursuivre un but légitime. En outre, il doit exister un rapport raisonnable de proportionnalité entre la différence de traitement et le but légitime recherché. Il s'ensuit que si les autorités répressives utilisent des profils larges qui reflètent des généralisations non examinées, leurs pratiques de surveillance ciblée peuvent constituer des ingérences disproportionnées dans les droits humains. En particulier, le profilage fondé sur des hypothèses stéréotypées selon lesquelles les personnes d'une certaine « race », d'une certaine origine nationale ou ethnique ou d'une certaine religion sont particulièrement susceptibles de commettre des délits peut conduire à des pratiques incompatibles avec le principe de non-discrimination. Si un ciblage sélectif a lieu, il doit être fondé sur le comportement individuel et non sur des caractéristiques innées ou sur l'appartenance à un groupe. *Voir* Agence des droits de l'Union européenne, *Guide pour la prévention du profilage illicite aujourd'hui et demain,* 5 décembre 2018, en particulier la section 2 sur « *Le profilage licite : principes et pratique* » ; voir également Réseau de l'UE d'experts indépendants en matière de droits fondamentaux, *Le profilage ethnique*, décembre 2006 ; Commission européenne contre le racisme et l'intolérance, *Recommandation de politique générale n° 11 de l'ECRI sur la lutte contre le racisme et la discrimination raciale dans les activités de la police*, 29 juin 2007 ; Comité pour l'élimination de la discrimination raciale, *Recommandation générale no 36 (2020) sur la prévention et l'élimination du recours au profilage racial par les répresentants de la loi*, 17 décembre 2020.

[27] Dans une juridiction au moins - le Royaume-Uni - il a été allégué que l'utilisation d'un logiciel espion avait causé un préjudice psychiatrique à sa victime, de sorte qu'il relevait d'une exemption à l'immunité souveraine et que des poursuites civiles pouvaient être engagées contre l'État étranger prétendument responsable (voir *Al Masarir c. Royaume d'Arabie saoudite [2023] 2 WLR 549*, 19 août 2022 *; Shehabi c. Royaume de Bahreïn [2024] EWCA Civ 1158*, 4 octobre 2024).

[28] Conseil de l'Europe, *Le logiciel espion Pegasus et ses répercussions sur les droits de l'homme* (« Rapport de la DGI sur le logiciel espions »), 2022, chapitre 5 : « [...] *La surveillance ciblée ou de masse crée également un climat d'autocensure. Craignant que chacun de leurs actes et mouvements ne soit scruté à la loupe, les personnes sont moins enclines à communiquer sur des sujets spécifiques en ligne ou hors ligne. L'effet paralysant de la surveillance peut également conduire à l'isolement social. Les cibles, ainsi que leurs parents et amis, pourraient s'abstenir de toute interaction, de peur d'être surveillés ou qu'on leur fasse du mal. Plus important encore, l'accès en temps réel aux données de localisation et de communication pourrait également mettre en danger l'intégrité physique et mentale des personnes, voire leur vie* [...] ».

[29] Pour la surveillance ciblée et secrète*, voir*, entre autres, CourEDH, *Roman Zakharov c. Russie* [GC], n° 47143/06, 4 décembre 2015 et Kennedy c. Royaume-Uni, n° 26839/05, 18 mai 2010. 47143/06, 4 décembre 2015 et *Kennedy c. Royaume-Uni*, no 26839/05, 18 mai 2010 ; pour les interceptions de masse*, voir* CEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], nos.58170/13 et 2 autres, 25 mai 2021 et *Centrum För Rättvisa c. Suède* [GC], no. 35252/08, 25 mai 2021.

[30] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 231.

d'exceptions[31]. Appliquant la jurisprudence susmentionnée, la CourEDH a récemment évalué la législation nationale polonaise sur la surveillance secrète et a constaté trois violations distinctes de l'article 8 de la CEDH[32].

19. En revanche, la surveillance de masse permet aux services de sécurité d'adopter une approche proactive, en recherchant des dangers jusqu'alors inconnus plutôt qu'en enquêtant sur des dangers connus. La CourEDH s'est penchée sur la question de l'interception de masse dans les affaires historiques *Big Brother Watch et autres c. Royaume-Uni* [GC] et *Centrum För Rättvisa c. Suède* [GC]. La CourEDH a estimé que l'interception de masse est « une capacité technologique précieuse pour identifier de nouvelles menaces dans le domaine numérique »[33] et qu'elle est d'une importance vitale pour les États contractants dans l'identification des menaces pour leur sécurité nationale[34]. Bien que l'article 8 de la CEDH n'interdise pas le recours à l'interception de masse pour protéger la sécurité nationale et d'autres intérêts nationaux essentiels contre des menaces extérieures graves, et que les États jouissent d'une large marge d'appréciation pour décider du type de régime d'interception nécessaire, à ces fins, le pouvoir discrétionnaire qui leur est accordé dans la mise en œuvre d'un tel système doit nécessairement être étroit et un certain nombre de garanties devront être mises en place[35].

20. En s'appuyant sur la jurisprudence de la CourEDH, on constate que, malgré les différences, il peut y avoir en pratique plusieurs chevauchements entre l'interception ciblée et l'interception de masse. Toute intrusion causée par l'acquisition de données de communication associées est multipliée par l'interception de masse, puisque ces données peuvent désormais être analysées et recherchées, ce qui permet de dresser un portrait intime de la personne concernée en suivant ses activités sur les réseaux sociaux, ses déplacements, ses habitudes de navigation sur internet et de communication, ainsi que ses contacts[36]. Les données en vrac peuvent être analysées afin d'identifier les dispositifs individuels présentant un intérêt, qui peuvent ensuite faire l'objet d'une interception ciblée.

21. La Commission de Venise s'est également penchée sur les questions de surveillance. En 2015, elle a mis à jour son rapport sur le contrôle démocratique des services de sécurité[37] et a produit un rapport sur le contrôle démocratique des agences de renseignement d'origine électromagnétique[38]. Le présent rapport doit donc être lu conjointement avec ces rapports, auxquels il sera fait référence dans la section V. La Commission de Venise a également adopté des avis sur les lois relatives à la surveillance ciblée[39].

---

[31] *Ibid*, §§ 286 et suivants, voir section V.H ci-dessous.
[32] CourEDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, n° 72038/17 et 25237/18, 28 mai 2024.
[33] CourEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], précité, § 323.
[34] *Ibidem*, § 424 ; *voir également* Commission de Venise, CDL-AD(2015)011, *Rapport sur le contrôle démocratique des agences de collecte de renseignement d'origine électromagnétique*, § 47.
[35] CourEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], précité au § 347. En particulier, la Cour a examiné si le cadre juridique national définissait clairement (i) les motifs pour lesquels l'interception de masse peut être autorisée ; (ii) les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ; (iii) la procédure à suivre pour accorder l'autorisation ; (iv) les procédures à suivre pour sélectionner, examiner et utiliser le matériel d'interception ; (v) les précautions à prendre lors de la communication du matériel à d'autres parties ; (vi) les limites de la durée de l'interception ; (vii) la durée de l'interception ; et (viii) la durée de l'interception ; (vi) les limites de la durée de l'interception, le stockage du matériel d'interception et les circonstances dans lesquelles ce matériel doit être effacé et détruit ; (vii) les procédures et modalités de contrôle par une autorité indépendante du respect des garanties susmentionnées et ses pouvoirs en cas de non-respect ; (viii) les procédures de contrôle indépendant a posteriori de ce respect et les pouvoirs conférés à l'organe compétent pour traiter les cas de non-respect, voir § 361.
[36] CourEDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, précité, § 249.
[37] Commission de Venise, CDL-AD(2015)010, *Rapport sur le contrôle démocratique des services de sécurité*.
[38] CDL-AD(2015)011, précité.
[39] *Voir, entre autres*, Commission de Venise, CDL-AD(2016)012, *Pologne - Avis relatif à la loi du 15 janvier 2016 portant modification de la loi sur la police et certaines autres lois*.

B. Protection des données personnelles

22. Bien que le droit à la protection des données à caractère personnel ne soit pas un droit autonome en vertu de la CEDH, la CourEDH a reconnu que la protection des données à caractère personnel revêt une importance fondamentale pour la jouissance par une personne de son droit au respect de la vie privée et familiale, du domicile et de la correspondance[40].

23. La Convention 108 du Conseil de l'Europe[41], le seul traité international juridiquement contraignant dans le domaine de la protection des données à caractère personnel ayant une portée mondiale, définit les principes de base de la protection des données, les garanties pour les personnes et le contrôle des opérations de traitement des données, qui sont particulièrement importants dans le contexte des technologies de surveillance, telles que les logiciels espions[42]. La Convention 108+ modernisée[43] a été ouverte à la signature et à la ratification en octobre 2018[44].

1. Principales exigences de la Convention 108+

24. La Convention 108+ établit des exigences plus strictes en ce qui concerne la licéité du traitement, la nécessité, la proportionnalité, la limitation de la finalité, la qualité des données et la minimisation des données, en rappelant que les données à caractère personnel traitées doivent être adéquates, pertinentes et non excessives. Le principe de proportionnalité s'applique également aux moyens et méthodes déployés pendant la surveillance. La Convention 108+ offre aux individus un plus grand contrôle sur leurs données personnelles et des droits renforcés[45]. En outre, il est précisé que l'exigence d'une base juridique valable pour le traitement s'applique en toutes circonstances, sans exception. Entre autres obligations, les responsables du traitement doivent mettre en œuvre les principes de « privacy by design » et de « privacy by default » dans le cadre du développement de produits ou de services[46] et doivent procéder à un examen prospectif de l'impact probable du traitement des données sur les droits humains et les libertés fondamentales.

25. Une exigence clé de la Convention 108+ et de la nouvelle génération de lois sur la protection des données est que les responsables du traitement des données à caractère personnel (y compris les services de renseignement et la police) et, le cas échéant, les sous-traitants (y compris les développeurs et les prestataires de services) doivent être en mesure de démontrer que le traitement des données à caractère personnel sous leur contrôle est conforme aux

---

[40] CourEDH, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, n° 931/13, 27 juin 2017, § 137.
[41] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108)
[42] Rapport de la DGI sur les logiciels espions, précité, p. 14.
[43] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel telle qu'elle sera amendée par son Protocole STCE n° 223.
[44] 31 pays ont à ce jour ratifié le Protocole d'amendement à la Convention 108. La Convention modernisée entrera en vigueur une fois ratifiée par l'ensemble des 55 Parties à la Convention 108 ou, à partir du 11 octobre 2023, une fois que 38 Parties à la Convention auront ratifié le Protocole.
[45] Dans son article 9, la convention modernisée élargit le catalogue des informations à transmettre aux personnes concernées lorsqu'elles exercent leur droit d'accès. En outre, les personnes concernées ont le droit d'obtenir la connaissance du raisonnement qui sous-tend le traitement des données dont les résultats lui sont appliqués. Le droit de ne pas faire l'objet d'une décision qui l'affecte de manière significative, prise sur le seul fondement d'un traitement automatisé, sans que l'avis de la personne concernée ne soit pris en considération. Enfin, les personnes concernées ont le droit de s'opposer à tout moment au traitement de leurs données à caractère personnel, à moins que le responsable du traitement ne démontre l'existence de motifs légitimes impérieux pour le traitement qui prévalent sur leurs intérêts ou leurs droits et libertés fondamentaux, *voir également* Conseil de l'Europe, *La Convention 108 modernisée : les nouveautés en un clin d'œil*.
[46] Le concept de « privacy by design » selon lequel la protection de la vie privée de chaque utilisateur doit commencer dès la conception des systèmes informatiques. Il a été codifié par le règlement (UE) 2016/679 (GDPR). Il permet une protection maximale des droits relatifs aux données à caractère personnel dès la conception et lors de chaque utilisation d'une nouvelle technologie. Ce principe implique que la protection des données personnelles n'est plus une option pour les entreprises mais une obligation inhérente à chacune de leurs activités.

principes (y compris la licéité, la limitation de la finalité, la minimisation des données, les limitations de stockage, la qualité des données) et aux obligations énoncés dans la Convention, y compris le respect de la vie privée dès la conception, le respect de la vie privée par défaut et l'évaluation de l'impact sur la protection des données. En outre, l'article 6 de la Convention 108+ prévoit que les données à caractère personnel qui révèlent l'origine raciale, les opinions politiques ou les convictions religieuses ou autres, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent faire l'objet d'un traitement automatisé que si le droit interne prévoit des garanties appropriées. Il en va de même pour les données à caractère personnel relatives aux condamnations pénales. Ainsi, cette disposition limite effectivement l'utilisation directe des critères énumérés dans les pratiques de surveillance, bien que l'utilisation de ces critères dans la surveillance ne soit pas toujours interdite. Par exemple, ces critères peuvent être appliqués à la surveillance ciblée lorsqu'il existe des renseignements spécifiques suggérant qu'une personne identifiable répondant à ces caractéristiques prépare un crime grave spécifique ou un acte constituant une menace grave pour la sécurité nationale.

26. L'évaluation de l'impact sur la vie privée (EIVP) prévue à l'article 10 § 2 de la Convention 108+ est essentielle dans le contexte des logiciels espions, car il s'agit d'un processus destiné à décrire le traitement des données à caractère personnel, à évaluer sa nécessité et sa proportionnalité, à identifier l'impact du traitement des données envisagé sur les droits et les libertés fondamentales des personnes concernées et à atténuer les risques découlant du traitement. Une analyse d'impact ne doit pas nécessairement indiquer que tous les risques ont été éradiqués, mais elle doit minimiser les risques autant que possible et le plus tôt possible, et évaluer si les risques résiduels sont justifiés.

27. L'exigence selon laquelle les motifs pour lesquels le traitement des données à caractère personnel est autorisé doivent être clairement et précisément définis par la loi est l'un des principes fondamentaux relatifs à la protection des données à caractère personnel. L'exigence de « qualité » de la loi peut également être tirée de l'article 11 de la Convention 108+ dans la mesure où il exige explicitement que les exceptions et les restrictions soient « prévues par la loi »[47].

28. Il découle de ces exigences que la législation donnant aux autorités le pouvoir de porter atteinte à la vie privée et aux données à caractère personnel en utilisant des logiciels espions et en traitant ensuite les données à caractère personnel obtenues par l'utilisation de logiciels espions doit contenir des dispositions explicites et détaillées concernant les personnes autorisées à consulter les données, la nature et la catégorie des données, la procédure à suivre ou l'utilisation qui peut être faite des informations ainsi obtenues. L'exigence de dispositions légales explicites et suffisamment détaillées et précises constitue également une garantie essentielle contre l'arbitraire et l'abus de pouvoir, ce qui revêt une importance particulière en ce qui concerne l'utilisation de logiciels espions, en raison du potentiel accru d'ingérence intrusive de ces technologies de surveillance.

2. Sécurité nationale et protection des données personnelles

29. Contrairement aux dispositions de la Convention 108, la Convention 108+ ne permet plus d'exclure entièrement du champ d'application de la convention le traitement de données pour des raisons liées à la sécurité (et à la défense) nationale (article 11). Les exceptions possibles à un nombre limité de principes (article 5, paragraphe 4, article 7, paragraphe 2, article 8, paragraphe 1, et article 9) sont soumises aux conditions fixées par la Convention. Ces exceptions doivent notamment (i) être prévues par la loi ; (ii) respecter l'essence des droits et libertés fondamentaux et (iii) constituer une mesure nécessaire dans une société démocratique sur la base de motifs précis et limités, notamment « la protection de la sécurité nationale, de la défense,

[47] Le paragraphe 91 du rapport explicatif de la Convention 108+ précise en outre qu'une telle mesure « *doit être établie par une loi accessible et prévisible qui doit être suffisamment détaillée* ».

de la sûreté publique, d'intérêts économiques et financiers importants de l'État, de l'impartialité et de l'indépendance du pouvoir judiciaire, ou la prévention, la recherche et la poursuite d'infractions pénales et l'exécution de sanctions pénales, ainsi que d'autres objectifs essentiels d'intérêt public général ».

30. En outre, en vertu de l'article 11, paragraphe 3, les activités de traitement à des fins de sécurité et de défense nationales doivent faire l'objet d'un examen et d'un contrôle indépendants et effectifs dans le cadre de la législation nationale de l'État partie concerné.

C. Travaux des institutions et tribunaux internationaux en matière de logiciels espions

31. Outre les travaux de l'APCE, un examen approfondi de l'utilisation de Pegasus et d'autres logiciels espions a été réalisé par le Parlement européen, qui a créé une commission d'enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (commission PEGA)[48]. La commission a produit une étude sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents[49], un rapport[50] et une recommandation au Conseil européen et à la Commission[51]. En 2019, le rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a publié un rapport sur la surveillance et les droits humains, qui mentionne le logiciel espion Pegasus comme un exemple de piratage d'appareils mobiles utilisé comme outil de surveillance ciblée dans 45 pays[52]. En 2022, le commissaire aux droits de l'homme des Nations Unies a estimé que l'utilisation de logiciels espions « *devrait se limiter aux cas où l'objectif est de prévenir une infraction grave ou un acte constituant une menace grave pour la sécurité nationale ou d'enquêter à ce sujet. Elle devrait aussi être étroitement circonscrite à l'enquête concernant la ou les personnes soupçonnées de commettre ou d'avoir commis de tels actes. Il doit s'agir d'une mesure de dernier ressort [...] toutes les mesures moins intrusives doivent avoir été épuisées ou s'être révélées inutiles − d'une portée et d'une durée strictement limitées. Seules les données pertinentes devraient être consultées et collectées. Toute mesure de ce type devrait également faire l'objet d'un contrôle indépendant rigoureux, et être soumise à l'approbation préalable d'un organe judiciaire. [...]* »[53] En 2023, le Commissaire aux droits de l'homme du Conseil de l'Europe a publié un commentaire appelant les États membres du Conseil de l'Europe à imposer un moratoire strict sur l'exportation, la vente, le transfert et l'utilisation de logiciels espions zéro-clic hautement intrusifs tels que Pegasus, et à mettre en place un cadre législatif précis et conforme aux droits humains pour l'utilisation des technologies de surveillance modernes[54].

---

[48] Parlement européen, *Décision du 10 mars 2022 sur la création d'une commission d'enquête chargée de faire la lumière sur l'utilisation du logiciel espion de surveillance Pegasus et de logiciels équivalents, et définissant l'objet de l'enquête, ainsi que les responsabilités, la composition numérique et la durée du mandat de la commission* (2022/2586(RSO)), 10 mars 2022.

[49] Étude PEGA, précitée.

[50] Rapport PEGA, précité.

[51] *Recommandation du Parlement européen du 15 juin 2023 au Conseil et à la Commission à la suite de l'enquête sur les allégations d'infractions et de mauvaise administration dans l'application du droit de l'Union en ce qui concerne l'utilisation de Pegasus et de logiciels espions de surveillance équivalents* (2023/2500(RSP)) (« Recommandation du PE »).

[52] Nations Unies, Assemblée générale, Conseil des droits de l'homme, A/HRC/41/35, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression* (« Rapport 2019 du RS des Nations Unies »), 28 mai 2019. *Voir également* le Rapporteur spécial des Nations Unies sur la promotion et la protection des droits humains et des libertés fondamentales dans la lutte antiterroriste, *Global Regulation of the Counter-Terrorism Spyware Technology Trade : Scoping Proposals for a Human-Rights Compliant Approach (Réglementation mondiale du commerce des technologies de lutte contre le terrorisme : propositions de cadrage pour une approche conforme aux droits humains)* (avril 2023).

[53] Conseil des droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, Rapport du Bureau du Haut Commissaire aux droits de l'homme des Nations Unies, A/HRC/51/17, 4 août 2022.

[54] Conseil de l'Europe, Commissaire aux droits de l'homme, *Des logiciels espions très intrusifs menacent l'essence des droits humains*, 27 janvier 2023.

32. Parmi les autres documents pertinents, on peut citer le rapport actualisé de 2023 de l'Agence des droits fondamentaux sur la « Surveillance par les services de renseignement »[55], qui met partiellement à jour les rapports de 2015 et 2017 de la même agence et fournit un examen complet des mécanismes de contrôle en place dans les pays de l'UE, et le rapport de 2022 du Conseil de l'Europe sur le logiciel espion Pegasus et son impact sur les droits humains[56].

33. En 2024, l'Acte européen pour la liberté des médias susmentionné, dans ses considérants 25 et 26, a établi certaines garanties qui doivent être respectées pour permettre l'utilisation légale de logiciels de surveillance intrusifs à l'encontre des fournisseurs de services de médias[57]. L'article 4, paragraphe 3, de l'Acte, conformément à la large protection des journalistes reconnue par le droit international des droits humains en tant que « chien de garde » public de la société démocratique, prévoit la norme par défaut selon laquelle les États membres doivent assurer la protection des sources journalistiques et des communications confidentielles et ne pas déployer de logiciels espions contre les professionnels des médias ou d'autres personnes qui pourraient entraîner la divulgation de sources et de communications. L'article 4 § 5 ne prévoit de dérogation à cette protection standard, c'est-à-dire au déploiement de logiciels de surveillance intrusifs, que dans des circonstances spécifiques (voir le paragraphe 95 ci-dessous).

34. La Cour de justice de l'Union européenne (CJUE) a également traité de l'utilisation des technologies de surveillance et de leur impact sur les droits fondamentaux dans un certain nombre d'affaires qui ont fait date[58].

---

[55] Rapport de la FRA, cité ci-dessus.

[56] Rapport de la DGI sur les logiciels espions, précité, p. 14.

[57] Les considérants 25 et 26 se lisent comme suit *(25) Les logiciels de surveillance intrusifs, y compris en particulier ce que l'on appelle communément les «logiciels espions», représentent une forme particulièrement invasive de surveillance des professionnels des médias et de leurs sources. Ils peuvent être déployés pour enregistrer secrètement des appels ou pour utiliser le microphone d'un appareil d'un utilisateur final, filmer ou photographier des personnes physiques, des machines ou leur environnement, copier des messages, accéder à des données relatives à des contenus chiffrés, suivre les activités de navigation, géolocaliser ou collecter d'autres données de capteurs, ou suivre les activités sur plusieurs appareils d'utilisateurs finaux. Ils ont des effets dissuasifs sur le libre exercice des activités économiques dans le secteur des médias. Ils compromettent, en particulier, la relation de confiance entre les journalistes et leurs sources, qui est essentielle à la profession de journaliste. Compte tenu de la nature numérique et intrusive de tels logiciels et de l'utilisation d'appareils par-delà les frontières, leur incidence est particulièrement néfaste sur l'exercice des activités économiques des fournisseurs de services de médias dans le marché intérieur. Il est donc nécessaire de veiller à ce que les fournisseurs de services de médias, y compris les journalistes, qui exercent leur activité dans le marché intérieur des services de médias puissent s'appuyer sur une protection harmonisée solide contre le déploiement de logiciels de surveillance intrusifs dans l'Union, y compris lorsque les autorités des États membres ont recours à des parties privées pour leur déploiement ;*
(26) Les logiciels de surveillance intrusifs ne devraient être déployés que lorsque cela est justifié par une raison impérieuse d'intérêt général, prévu par le droit de l'Union ou le droit national, conforme à l'article 52, paragraphe 1, de la charte, tel qu'il est interprété par la Cour de justice, et à d'autres dispositions du droit de l'Union, autorisé ex ante ou, dans des cas exceptionnels et urgents, confirmé ultérieurement par une autorité judiciaire ou une autorité décisionnelle indépendante et impartiale, s'il intervient dans le cadre d'enquêtes relatives à des infractions énumérées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil (9) passibles dans l'État membre concerné d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans, ou d'une enquête relative à d'autres infractions graves passibles dans l'État membre concerné d'une peine ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins cinq ans, conformément au droit national de cet État membre, et à condition qu'aucune autre mesure moins restrictive ne soit adéquate et suffisante pour obtenir les informations recherchées. Conformément au principe de proportionnalité, des limitations ne peuvent être apportées aux droits et libertés d'un individu que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union. Ainsi, s'agissant spécifiquement du déploiement d'un logiciel de surveillance intrusif, il convient de s'assurer que l'infraction en cause atteint un seuil de gravité, comme le prévoit le présent règlement, qu'à la suite d'une appréciation individuelle de toutes les circonstances pertinentes d'une affaire donnée, l'enquête et les poursuites relatives à cette infraction justifient, l'ingérence particulièrement intrusive dans les droits fondamentaux et les libertés économiques au moyen d'un logiciel de surveillance intrusif, qu'il existe des preuves suffisantes que l'infraction en question a été commise et que le déploiement d'un logiciel de surveillance intrusif est pertinent aux fins de l'établissement des faits liés à l'enquête et aux poursuites relatives à cette infraction.

[58] Entre autres, CJUE, *Digital Rights Ireland et Seitlinger et autres*, affaires jointes C-293/12 et C-594/12, 8 avril 2014 ; *Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson et autres*, affaires jointes C-203/15 et C-698/15, 21 décembre 2016 ; *Maximillian Schrems contre Data*

IV. Conclusions comparatives concernant la législation et la pratique en matière de logiciels espions

35. Afin de mener une étude comparative sur le cadre législatif de ses Etats membres concernant l'utilisation de logiciels espions, la Commission de Venise s'est basée sur les garanties développées par la CourEDH dans sa jurisprudence sur la surveillance ciblée[59]. En particulier, elle a demandé à ses membres de fournir des informations sur les points suivants (i) si les cadres juridiques nationaux autorisent l'utilisation de logiciels espions comme outil de surveillance ciblée dans le cadre d'enquêtes criminelles ou de renseignement ; (ii) s'il existe des règles spécifiques (couvrant notamment le champ d'application ratione *materiae*, *temporis* et *personae*) ou si les règles générales sur la surveillance ciblée (interception des communications) s'appliquent ; (iii) le type de données, le cas échéant, qui pourraient être collectées à l'aide de logiciels espions ; (iv) l'existence d'une autorité officielle ou d'une autorité de contrôle de l'utilisation des logiciels espions ; (v) l'existence d'une autorité de contrôle de l'utilisation des logiciels espions ; (iv) l'existence d'une évaluation officielle de la nécessité ou de la valeur ajoutée des logiciels espions ; (v) les organes chargés d'autoriser/approuver les mesures de surveillance ciblée dans les enquêtes criminelles et de renseignement ; (vi) les mécanismes nationaux de contrôle en place pour les activités des services de sécurité ; et (vii) l'existence d'un mécanisme de notification post-surveillance ou de tout autre recours.

36. Les exemples cités ne sont pas exhaustifs et sont uniquement basés sur les données disponibles, notamment les réponses fournies au questionnaire et les informations qui ont été recueillies par ailleurs par les rapporteurs. En outre, la Commission de Venise rappelle que les exemples cités dans le rapport ne sont présentés qu'à des fins de comparaison et non pour approuver une approche particulière.

A. Base juridique de l'utilisation de logiciels espions comme outil de surveillance ciblée

37. Sur la base des garanties susmentionnées, la Commission de Venise a tout d'abord examiné le cadre juridique existant pour l'utilisation des logiciels espions dans ses Etats membres. Il est apparu que relativement peu d'États ont élaboré une législation qui réglemente spécifiquement l'utilisation d'outils de surveillance intrusifs/de logiciels espions : **Canada**, **Danemark**, **Finlande**, **Allemagne**, **Italie**, **Luxembourg**, **Pays-Bas**, **Norvège**, **Espagne**, **Suède**, **Suisse** et **Royaume-Uni.** En **Autriche**, la législation sur l'utilisation des logiciels espions avait été initialement introduite dans le cadre d'enquêtes criminelles. Cependant, elle a ensuite été annulée par la Cour constitutionnelle qui a estimé qu'elle constituait une ingérence disproportionnée dans les droits

Protection Commissioner, affaire C-362/14, 6 octobre 2015 ; *Privacy International contre Secretary of State for Foreign and Commonwealth Affairs et autres*, affaire C-623/17, 6 octobre 2020 ; *La Quadrature du Net et autres c. Premier ministre et autres*, affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020. Les rapports de la FRA de 2015, 2017 et 2023 comprennent des listes complètes des arrêts de la Cour de justice de l'Union européenne sur les questions de surveillance. Un récent arrêt de la Grande Chambre de la CJUE (*CG c. Bezirkshauptmannschaft Landeck*, affaire C-548/21, 4 octobre 2024) portait sur l'accès par la police aux données contenues dans un téléphone portable, une ingérence connexe mais moins intrusive avec le déploiement d'un logiciel de surveillance intrusif. Tout en reconnaissant que les données à caractère personnel stockées sur un téléphone portable peuvent constituer une ingérence particulièrement grave dans les droits fondamentaux de la personne concernée, la Cour a estimé que le fait de considérer que seule la lutte contre la criminalité grave peut justifier l'accès aux données contenues dans un téléphone portable limiterait indûment les pouvoirs d'enquête des autorités compétentes. Il en résulterait un risque accru d'impunité pour les infractions pénales en général et donc un risque pour la création d'un espace de liberté, de sécurité et de justice dans l'Union européenne. La Cour a néanmoins estimé qu'une telle ingérence dans la vie privée et la protection des données doit être prévue par la loi, ce qui implique que le législateur national définisse les éléments à prendre en compte pour un tel accès, tels que la nature ou les catégories d'infractions concernées. Afin d'assurer le respect du principe de proportionnalité dans chaque cas concret, l'accès aux données doit être soumis à l'autorisation préalable d'un tribunal ou d'une autorité indépendante, sauf en cas d'urgence dûment justifiée. Enfin, la personne concernée doit être informée des motifs de l'autorisation dès que la fourniture de cette information n'est plus susceptible de compromettre les enquêtes.

[59] Voir le paragraphe 18 ci-dessus.

humains[60]. Dans certains des États susmentionnés, des règles spécifiques (*ratione materiae, ratione personae et ratione temporis*), qui s'écartent du cadre général en place pour les mesures de surveillance ciblée, ont été mises en place (voir ci-dessous la section IV.C). En **Belgique**, en **Bulgarie**, en **Estonie**, en **France**, en **Hongrie**, en **Lituanie**, en **République de Moldova**, en **Macédoine du Nord**, en **Pologne**, en **Roumanie** et en **République slovaque**, l'utilisation de logiciels espions, bien qu'elle ne fasse pas l'objet d'une réglementation distincte et autonome, serait autorisée dans le cadre de la notion de « moyens techniques spéciaux/mesures d'enquête spéciales ». Dans les pays qui n'ont pas de législation spécifique sur les logiciels espions, sur la base des informations disponibles, lorsque l'utilisation de logiciels espions n'est pas expressément interdite à *première vue*, il est possible que les règles générales sur la surveillance ciblée s'appliquent et que les logiciels espions soient considérés comme une méthode permettant d'obtenir des données pertinentes, sans règles spécifiques. Bien qu'elle ne soit pas spécifiquement réglementée, la jurisprudence des tribunaux des **États-Unis** montre que le déploiement national de toute technologie de surveillance devrait être régi par des exigences strictes en matière de mandat et que son utilisation devrait avoir un champ d'application restreint[61].

38. La législation en vigueur dans les pays qui réglementent spécifiquement les logiciels espions est pour la plupart antérieure aux révélations « Pegasus ». Ce n'est qu'en **Grèce** qu'une législation spécifique a été introduite à la suite des révélations sur l'utilisation abusive des logiciels espions, prévoyant*, entre autres,* un nouveau cadre juridique pour la levée de la confidentialité des communications et autorisant l'achat de logiciels espions par les autorités de l'État[62].

39. Dans les pays où l'utilisation des logiciels espions est explicitement réglementée, ils peuvent normalement être utilisés à la fois par les agents chargés de l'application de la loi dans le cadre d'enquêtes criminelles et par les agences de sécurité dans le cadre d'enquêtes de renseignement visant à prévenir les menaces pour la sécurité nationale[63]. L'autorisation légale d'utiliser des logiciels espions se trouve parfois dans la même loi, parfois dans des lois distinctes.

---

[60] *Voir le* paragraphe 70 ci-dessous.

[61] Le quatrième amendement de la Constitution des États-Unis constitue le fondement du cadre juridique américain régissant la surveillance dans le système de justice pénale. L'arrêt *Carpenter v. United States, rendu* en 2018 par la Cour suprême, a fait date en déclarant inconstitutionnelle l'utilisation sans mandat d'informations relatives à la localisation de sites cellulaires, offrant ainsi aux individus une protection contre la recherche par le gouvernement de données personnelles auprès de tiers. *Carpenter* a fourni une série de facteurs permettant d'évaluer la constitutionnalité de telles pratiques de surveillance lorsqu'elles sont menées sans mandat judiciaire, y compris des facteurs particulièrement pertinents pour les logiciels espions, tels que la nature révélatrice des informations collectées et la quantité de données recherchées par le gouvernement. Des juridictions inférieures ont estimé que les protections du quatrième amendement limitent l'utilisation par le gouvernement de technologies qui peuvent être similaires aux logiciels espions tels que définis ci-dessus. Par exemple, dans l'*affaire United States v. Wilson*, la Cour d'appel des États-Unis pour le neuvième circuit a estimé que l'installation par les forces de l'ordre d'un logiciel malveillant de surveillance sur l'ordinateur d'un prévenu sans mandat constituait une perquisition et une saisie illégales. Dans l'affaire *United States v. Saboonchi*, les tribunaux ont estimé que l'utilisation par les forces de l'ordre d'un logiciel malveillant pour activer à distance la webcam de l'ordinateur portable du défendeur constituait une perquisition inconstitutionnelle. Ces affaires permettent de conclure que les logiciels espions, compte tenu de leur caractère intrusif, seraient probablement régis de manière stricte par les exigences du mandat et l'étendue de l'utilisation. Cela dit, l'applicabilité générale de la loi à la surveillance numérique est peut-être en train de changer. Par exemple, dans l'affaire *Tuggle v. United States*, une cour d'appel a estimé que l'utilisation à long terme d'une caméra placée sur un poteau pour surveiller le domicile d'une personne était raisonnable au regard du quatrième amendement.

[62] L'utilisation de logiciels espions par les agences de l'État peut être autorisée, en vertu d'un décret présidentiel qui n'a pas encore été publié à ce jour (article 13 de la loi 5002 de 2022).

[63] En Italie, la loi ne fait pas explicitement référence à la possibilité d'utiliser des logiciels espions comme moyen d'effectuer des interceptions de renseignements ; certains auteurs, par voie d'interprétation, admettent toutefois cette possibilité ; en Norvège, le service de renseignement ne peut pas utiliser la surveillance ciblée, ou d'autres formes de surveillance, sur des personnes en Norvège ; en Espagne, il n'existe pas de réglementation spécifique sur l'utilisation de logiciels espions (y compris Pegasus) par les services de renseignement.

40. Parmi les pays qui autorisent l'utilisation de logiciels espions, on ne dispose pas de données sur l'outil exact utilisé par les autorités[64], en particulier pour savoir si des logiciels espions commerciaux sont utilisés ou si l'État a développé ses propres outils. Les États disposant d'une grande expérience et de ressources importantes dans le domaine du renseignement d'origine électromagnétique sont susceptibles d'avoir développé leurs propres outils. Sur la base des réponses reçues, la Commission de Venise a pu observer ce qui suit : aux **Pays-Bas**, le Centre de recherche et de données du ministère néerlandais de la Justice et de la Sécurité a publié un rapport d'évaluation sur les pouvoirs de surveillance néerlandais pour les autorités chargées de l'application de la loi ; ce rapport précise que la police néerlandaise a utilisé un outil commercial dans la « grande majorité » des cas. Ce rapport précise que la police néerlandaise a utilisé un outil commercial dans la « grande majorité » des cas. Toutefois, le nom de l'outil commercial utilisé n'est pas public. En **Suisse**, le Tribunal administratif fédéral, dans un arrêt du 9 janvier 2022[65], statuant sur le recours d'un avocat qui demandait l'accès au contrat relatif au logiciel espion utilisé par l'Office fédéral de la police et le Service de renseignement de la Confédération, a déclaré qu'il existe un intérêt public important à déterminer si le logiciel acquis par la Suisse est Pegasus. La Cour a estimé que la connaissance des informations demandées pourrait mettre en péril les mesures prises par la Suisse en cas de menace concrète pour sa sécurité intérieure et extérieure, ce qui entraverait à son tour le travail des autorités chargées de l'application de la loi.

B. Type d'informations susceptibles d'être collectées par les logiciels espions

41. La Commission de Venise a également recueilli des informations sur le type de données pouvant être collectées par des logiciels espions dans les pays qui les réglementent spécifiquement. Au **Canada**, les données pouvant être collectées sont limitées aux communications privées, aux données de transmission et/ou à l'acquisition de données statiques à partir d'appareils électroniques. Au **Danemark**, la loi ne prévoit aucune limitation spécifique à cet égard. En **Finlande**, la loi n'autorise pas la surveillance technique pour la collecte d'informations sur les communications en direct ou sur leurs données d'identification[66]. En **Allemagne**, le champ d'application des « infiltrations techniques/perquisitions en ligne » (telles que définies par la Cour constitutionnelle fédérale) a été considérablement limité à la suite d'un arrêt de principe de la Cour constitutionnelle fédérale (décision BvR 370/07)[67]. En particulier, l'article 100d du code de procédure pénale et l'article 49 § 7 de la loi sur l'Office fédéral de police criminelle prévoient que si des éléments factuels permettent de supposer qu'une mesure de recherche en ligne ne conduira qu'à des découvertes dans le domaine essentiel de la vie privée, la mesure est irrecevable. En outre, dans la mesure du possible, des mesures techniques doivent être prises pour garantir que les données relatives au domaine essentiel de la vie privée ne sont pas collectées. Depuis la loi de juillet 2021 visant à adapter la loi de protection constitutionnelle

[64] Dans les pays où ils sont utilisés, les logiciels espions portent des noms différents : logiciel/programme en Finlande (section 42 de la loi sur les mesures coercitives et section 42 de la loi sur le renseignement militaire), en Norvège (article 216 p de la loi sur la procédure pénale) et en Espagne (chapitre IX, titre VIII du code de procédure pénale) ; intercepteur informatique en Italie (« *captatore informatico* », tel que défini à l'article 1(m) du décret ministériel du 6 octobre 2022 comme « *tout système déguisé, inoculé à distance, qui, en éliminant les effets qui empêchent la connaissance de la communication ou des données, permet l'interception des contenus audio-vidéo et des données échangées ou permet l'interception des conversations face à face, et recueille à distance les positions prises par l'équipement sur le territoire* ») ; outil/implant d'enquête sur dispositif au Canada ; dispositif technique aux Pays-Bas (règlement sur les dispositifs techniques dans le droit de la procédure pénale publié le 11 juillet 2018 et article 45 de la loi néerlandaise sur les services de sécurité et de renseignement) ; « logiciel gouvernemental » ou « GovWare » en Suisse (comme indiqué dans le rapport explicatif du gouvernement sur les modifications du Code pénal suisse).

[65] Disponible ici ; le jugement n'est pas encore définitif - l'affaire est pendante devant le Tribunal fédéral.

[66] Article 23 § 2 de la loi sur les mesures coercitives, article 23 § 2 de la loi sur la police et article 32 § 2 de la loi sur le renseignement militaire.

[67] BVerfG, arrêt du premier sénat du 27 février 2008 - 1 BvR 370/07 -, (traduction anglaise), paragraphes 166 et suivants. Ce pouvoir est toutefois limité à la surveillance des communications et ne permet pas d'accéder à d'autres informations sur le disque dur ou dans le nuage. Le logiciel utilisé doit être strictement limité à la surveillance des communications.

(*Gesetz zur Anpassung des Verfassungsschutzrechts*), les 19 services de renseignement allemands ont le droit d'utiliser des chevaux de Troie pour lire les communications en cours sur les ordinateurs ou les smartphones et même les données de communication antérieures[68]. En **Italie**, bien que le logiciel de surveillance intrusif ait un potentiel de grande intrusion[69], le Parlement italien n'a expressément réglementé l'utilisation de cet outil d'investigation que pour l'interception de conversations en face-à-face et uniquement sur des appareils mobiles. Au **Luxembourg**, la police peut utiliser des logiciels espions pour capturer des données informatiques, tandis que les services de sécurité peuvent rechercher, de manière ciblée, des informations nécessaires à l'accomplissement de l'une de leurs missions, ou surveiller et contrôler des communications qui ne peuvent pas être techniquement interceptées en utilisant les réseaux de télécommunications normaux[70]. Aux **Pays-Bas**, la loi ne définit pas les données qui peuvent être collectées par les autorités chargées de l'application de la loi, mais se réfère plutôt aux méthodes par lesquelles les données peuvent être collectées ou modifiées[71]. Le Service général de renseignement et de sécurité et le Service militaire de renseignement et de sécurité sont autorisés à intercepter, recevoir, enregistrer et écouter toute forme de conversation, de télécommunication ou de transmission de données à l'aide d'un outil technique par le biais d'un travail automatisé, quel que soit l'endroit où il se trouve. Cette autorité comprend également le pouvoir de décrypter des conversations, des télécommunications ou des transmissions de données[72]. En **Norvège**, la lecture peut inclure des communications, des données stockées électroniquement et d'autres informations relatives à l'utilisation du système informatique ou du compte d'utilisateur[73]. En **Espagne**, l'article 588 *septies*(a) du code de procédure pénale prévoit qu'un logiciel peut être installé pour examiner le contenu d'un ordinateur, d'un dispositif électronique, d'un système informatique, d'un instrument de stockage de données de masse ou d'une base de données, à l'insu du propriétaire ou de l'utilisateur. En **Suède**, les logiciels espions peuvent être utilisés non seulement pour intercepter des données ou pour surveiller les communications et les informations de localisation, mais aussi pour effectuer une surveillance audio et par caméra[74]. En **Suisse**, l'utilisation de logiciels espions dans le cadre de procédures pénales est sans équivoque limitée à l'interception et à la récupération du contenu des

[68] Étude PEGA, citée ci-dessus, § 4.5.

[69] L'outil utilisé est potentiellement capable d'intercepter les communications entre les ordinateurs et les systèmes télématiques (courriels, messages WhatsApp, conversations Skype, etc.), d'activer les microphones et/ou les caméras et le GPS, d'enregistrer tout ce qui est tapé sur le clavier (fonction dite de keylogging) et tout ce qui apparaît à l'écran (fonction dite de capture d'écran). Il peut également s'infiltrer dans la mémoire des appareils où sont stockées des données, capturant ainsi toutes les données et informations contenues dans l'appareil infecté ou transitant par celui-ci, et modifiant toute information stockée ou transmise.

[70] Article 8 § 1(c) de la loi SRE.

[71] Ces méthodes comprennent : (i) la détermination des caractéristiques du travail automatisé ou de l'utilisateur, telles que l'identité ou la localisation ; (ii) l'exécution du pouvoir spécial d'investigation que constitue l'interception ciblée. Il est possible d'intercepter des communications, telles que le courrier électronique ou la parole, à l'aide d'un dispositif technique (y compris un logiciel). Ce point est détaillé dans le rapport explicatif de la loi sur la criminalité informatique III (par exemple, Série parlementaire II 2015-2016, 34372, no. 3, p. 9) ; (iii) l'exécution du pouvoir d'enquête spécial d'observation systématique, par exemple, pour déterminer l'emplacement du dispositif utilisé (par exemple, Série parlementaire II 2015-2016, 34372, no. 3, p. 9) ; (iv) l'exécution du pouvoir d'enquête spécial d'observation systématique, par exemple, pour déterminer l'emplacement du dispositif utilisé (par exemple, Série parlementaire II 2015-2016, 34372, no. 3, p. 14) ; (iv) enregistrer les données stockées dans le travail automatisé ; (v) rendre les données inaccessibles, telles que les documents relatifs à la maltraitance des enfants (Série parlementaire II 2015-2016, 34372, no. 3, p. 29), cfr. Article 126nba(1)(a) du Code de procédure pénale néerlandais.

[72] Articles 47(1) et 45(2)(b)(d) de la loi sur les services de sécurité et de renseignement,

[73] Article 216 o § 4. Il convient de noter la disposition selon laquelle la lecture des données doit être organisée de manière à ce qu'aucune information ne soit inutilement recueillie sur l'utilisation du système informatique par une personne autre que le suspect. La lecture doit être effectuée de telle sorte qu'il n'y ait pas de risque inutile de perturbation opérationnelle ou de dommage à l'équipement ou aux données. La police doit, dans la mesure du possible, prévenir le risque que la mise en œuvre permette à quelqu'un d'accéder sans autorisation au système informatique ou à des informations protégées, ou de commettre d'autres actes criminels.

[74] Cfr. Section 2 de la loi (2020:62) sur la lecture des données secrètes. Les statistiques publiées par le procureur général montrent toutefois que l'autorisation d'activer à distance la vidéosurveillance d'un appareil n'a été accordée que quatre fois en 2023. L'autorisation d'activer à distance la surveillance audio d'un appareil n'a également été donnée que quatre fois en 2023.

communications et des métadonnées de télécommunications sous forme non codée[75]. Il n'y a pas de limitations apparentes en ce qui concerne les données collectées dans les procédures de renseignement ; cependant, l'article 26 § d de la loi fédérale suisse du 25 septembre 2015 sur le service de renseignement (« IntelSA ») prévoit que l'intrusion dans les systèmes et réseaux informatiques peut être effectuée non seulement pour recueillir des informations qui y sont disponibles ou qui sont transmises à partir de ces systèmes et réseaux, mais aussi pour perturber, empêcher ou ralentir l'accès aux informations lorsque les systèmes et réseaux informatiques sont utilisés pour des attaques contre des infrastructures critiques. Au **Royaume-Uni**, l'article 99 § 2 de l'Investigatory Powers Act 2016 prévoit que les communications, les données d'équipement ou toute autre information peuvent être obtenues par le biais d'un mandat d'interférence ciblée de l'équipement.

42. Dans plusieurs des pays qui utilisent des logiciels espions, les données protégées par le secret professionnel d'un avocat ou d'un médecin, ou par le secret des sources d'un journaliste ne peuvent être collectées ou analysées, ou des procédures spécifiques sont en place[76].

C. Règles spécifiques *ratione materiae, personae et temporis* dans les États qui réglementent l'utilisation des logiciels espions

43. Comme indiqué ci-dessus, certains États ont élaboré des règles spécifiques pour l'utilisation d'outils de surveillance intrusifs tels que les logiciels espions et ont adapté en conséquence les conditions d'utilisation de ces outils par les services répressifs et de renseignement, notamment en ce qui concerne l'applicabilité *ratione materiae* et *temporelle* de la mesure de surveillance.

[75] Article 269ter du code de procédure pénale.

[76] Voir par exemple en Belgique l'article 18/9 § 4 de la L. R&S qui stipule qu'une méthode exceptionnelle ne peut être utilisée à l'encontre d'un avocat, d'un médecin ou d'un journaliste, ou des moyens de communication qu'ils utilisent à des fins professionnelles, que si le service de renseignement et de sécurité dispose d'indices préalables sérieux selon lesquels l'avocat, le médecin ou le journaliste est ou a été personnellement et activement impliqué dans la création ou le développement d'une menace potentielle grave. L'article 2 § 2 de la loi interdit toutefois aux services de renseignement et de sécurité d'obtenir, d'analyser ou d'exploiter des données protégées par le secret professionnel d'un avocat ou d'un médecin, ou par le secret des sources d'un journaliste ; en Finlande, l'article 82 de la loi sur le renseignement militaire prévoit que l'interception des télécommunications, la collecte de données autrement que par l'interception des télécommunications, l'interception sur place, l'observation technique, le renseignement sur les signaux radio ou le renseignement sur le trafic réseau ne doivent pas viser des communications ou des informations pour lesquelles une partie ne peut pas témoigner ou a le droit de refuser de témoigner (secret professionnel dans la relation entre un avocat et son client, privilège du clergé et privilège du médecin). Des dispositions similaires figurent dans la loi sur les mesures coercitives et la loi sur la police. Au Luxembourg, l'article 88-2, paragraphe 6, alinéa 3, prévoit que l'installation du dispositif technique mentionné aux paragraphes 2 et 3 de l'article 88-1 ne peut, sous peine de nullité, être effectuée dans les locaux à usage professionnel, le domicile ou ses dépendances au sens des articles 479, 480 et 481 du code pénal, ou le véhicule d'un avocat, d'un médecin, d'un journaliste professionnel ou d'un éditeur. Aux Pays-Bas, une procédure spéciale est prévue si la mesure de renseignement est mise en œuvre à l'encontre d'un journaliste ou d'un avocat (article 30 de la loi de 2017 sur les services de renseignement et de sécurité). Si la mesure de surveillance est utilisée contre un journaliste et que cela peut conduire à ce que l'identité d'une source du journaliste soit révélée au service de renseignement et de sécurité, l'autorisation pour l'exercice de ce pouvoir doit être accordée par le tribunal de district de La Haye, plutôt que par le ministre. Le tribunal appliquera les mêmes critères que le ministre, y compris le respect des principes de nécessité, de proportionnalité et de subsidiarité. Le tribunal peut autoriser l'exercice du pouvoir pour une période maximale de quatre semaines, au lieu de la limite habituelle de trois mois. En Suède, la loi 2020:62 sur la lecture de données secrètes (§ 11) interdit l'utilisation de la surveillance ciblée au moyen de logiciels espions sur les ordinateurs ou les téléphones des journalistes, des avocats, des médecins ou des prêtres ; en Suisse, l'article 271 du code de procédure pénale prévoit que Dans le cas de la surveillance d'une personne appartenant à l'une des catégories professionnelles énumérées aux articles 170 à 173, le tri des informations peut être effectué par l'intermédiaire d'un logiciel espion ou d'un logiciel de surveillance. 170 à 173, le tri des informations qui ne sont pas pertinentes pour l'objet de l'enquête ou pour la raison pour laquelle la personne concernée est surveillée doit être effectué sous la direction d'un tribunal. Ce tri est effectué de manière à ce que les autorités de poursuite ne soient pas informées des secrets professionnels. Les données écartées doivent être détruites immédiatement ; elles ne peuvent pas être utilisées. Le tri préalable des informations visé à l'al. 1 ne doit pas être effectué : a. s'il existe de sérieux soupçons à l'encontre du détenteur du secret professionnel, et b. s'il existe des raisons particulières de le faire. Des dispositions similaires figurent à l'article 58 de la loi fédérale du 25 septembre 2015 sur le service de renseignement (« LRens ») pour les surveillances ciblées effectuées par les services de sécurité.

Cette section donne un aperçu de ces règles spécifiques dans les pays qui ont signalé l'utilisation de logiciels espions.

1. *Ratione materiae*

44. Au **Danemark**, l'enquête doit porter sur une infraction punie par la loi d'une peine d'emprisonnement de six ans ou plus ou sur une violation intentionnelle du chapitre 12 ou 13 du code pénal[77].

45. En **Allemagne**, c'est la liste plus restreinte de crimes prévue à l'article 100b du code de procédure pénale qui s'applique (plutôt que celle prévue à l'article 100a). Dans le cadre des enquêtes de renseignement, l'Office fédéral de police criminelle ne peut accéder aux systèmes informatiques que si certains faits justifient l'hypothèse d'un danger pour (i) le corps, la vie ou la liberté d'une personne ou (ii) de tels biens publics, dont la menace affecte les fondements ou l'existence de la fédération ou d'un pays ou les fondements de l'existence humaine[78].

46. En **Italie**, les logiciels espions ne peuvent être utilisés dans le cadre de procédures pénales que pour des infractions particulièrement graves (telles que, par exemple, les associations criminelles de type mafieux)[79] ou, à condition que les lieux et les moments auxquels les logiciels espions peuvent être activés soient déterminés, même indirectement, également pour des infractions commises par des fonctionnaires contre l'administration publique et pour lesquelles une peine maximale d'au moins cinq ans d'emprisonnement est prévue[80].

47. Au **Luxembourg**, les logiciels espions ne peuvent être utilisés dans le cadre de procédures pénales que lorsqu'il s'agit de crimes graves, y compris les atteintes à la sûreté de l'État[81] et les actes de terrorisme et de financement du terrorisme ;[82] dans le cadre d'enquêtes de renseignement, les logiciels espions ne peuvent être utilisés qu'en présence d'une menace ou d'un risque de menace pour la sûreté de l'État[83].

48. Aux **Pays-Bas**, le législateur a prévu différentes exigences en ce qui concerne le degré d'intrusion de la mesure demandée, par rapport à la gravité des infractions. Pour trois catégories de méthodes permettant de collecter ou de modifier des données[84], la mesure peut être demandée en cas de suspicion d'une infraction grave pour laquelle la détention provisoire est autorisée (principalement les infractions passibles d'une peine d'au moins quatre ans). Deux autres méthodes plus intrusives peuvent être utilisées[85] uniquement pour les infractions punies d'une peine d'au moins huit ans ou désignées comme une infraction par la loi dans le décret sur

[77] Article 791(b) de la loi sur l'administration de la justice.
[78] Article 49 § 1 de la loi sur l'Office fédéral de police criminelle.
[79] Article 51 § *3-bis* et *3-quater* du code de procédure pénale.
[80] Dans la première phase d'application, les logiciels espions n'avaient été introduits qu'en référence aux crimes les plus graves de la criminalité organisée et du terrorisme ; l'extension en 2019 aux infractions contre l'administration publique a fait l'objet de diverses critiques, au regard du principe de proportionnalité nécessaire, *voir* Senato della Repubblica, *Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, précité, p. 43.
[81] Comme le prévoient les articles 101 à 123 du code pénal.
[82] Comme le prévoient les articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du code pénal.
[83] La loi précise à l'article 8 § 1(c) la nature des menaces potentielles pour la sécurité nationale : (i) espionnage et ingérence ; (ii) extrémisme violent ; (iii) terrorisme ; (iv) prolifération d'armes de destruction massive ou de produits et technologies liés à la défense ; (v) criminalité organisée et cyber-menaces, dans la mesure où elles sont liées à l'une des menaces susmentionnées. La loi exclut explicitement la surveillance politique interne des attributions du service de sécurité. Le champ de cette mission s'étend également à la sécurité des États étrangers et des organisations internationales et supranationales avec lesquelles le Luxembourg a signé des accords.
[84] En vertu de l'article 126nba § 1(a) : (i) identification et enregistrement de certaines caractéristiques du système informatique ou de la personne qui l'utilise, telles que l'identité et la localisation du système informatique ; (ii) ordre d'enregistrement des communications suite à une pénétration ; (iii) ordre de surveillance systématique.
[85] (iv) la capture des données stockées dans le système informatique ; et (v) les données peuvent être rendues inaccessibles, y compris leur effacement (temporaire).

les enquêtes dans un système informatique[86] sont envisagées. Les services de renseignement peuvent utiliser des logiciels espions lorsque les cibles (individus ou organisations) constituent une menace pour la sécurité nationale ou l'ordre démocratique des Pays-Bas[87].

49. En **Norvège**, la possibilité d'utiliser des logiciels espions est limitée aux délits très graves, c'est-à-dire aux délits passibles d'une peine de plus de 10 ans d'emprisonnement[88].

50. En **Espagne**, ce type de mesure n'est autorisé que pour des infractions spécifiques (infractions commises par des organisations criminelles, terrorisme, infractions contre des mineurs ou des personnes handicapées, infractions contre la constitution, trahison ou atteinte à la défense nationale, infractions commises à l'aide d'outils informatiques)[89].

51. En **Suède**, il existe une distinction entre la lecture de données n'impliquant pas l'activation du microphone d'un appareil pour enregistrer du son et celle impliquant l'activation du microphone d'un appareil pour enregistrer du son. Dans le premier cas, une liste assez large d'infractions pour lesquelles l'interception des communications est autorisée s'applique[90]. Pour la lecture de données secrètes impliquant l'activation du microphone de l'appareil pour enregistrer le son, la liste des infractions autorisées est beaucoup plus courte : seules celles punies d'une peine minimale de quatre ans d'emprisonnement, ainsi qu'un petit nombre d'infractions liées à la sécurité (espionnage, etc.) punies d'une peine minimale moins élevée[91].

52. En **Suisse**, les logiciels espions ne peuvent être utilisés dans le cadre de procédures pénales que pour la liste restreinte d'infractions relatives aux enquêtes secrètes, conformément à l'article 286, paragraphe 2, du CPP (pour les autres mesures de surveillance ciblée, la liste plus large de l'article 269 s'applique). Dans les enquêtes de renseignement, l'article 27 de la loi sur le renseignement limite la possibilité de recueillir des informations aux cas spécifiques mentionnés à l'article 19, paragraphe 2, points a) et d), ou à la sauvegarde d'autres intérêts nationaux importants.

53. Au **Royaume-Uni**, un mandat d'interférence thématique ciblée ne peut être délivré que : (i) dans l'intérêt de la sécurité nationale, (ii) dans le but de prévenir ou de détecter des crimes graves ou (iii) dans l'intérêt du bien-être économique du Royaume-Uni, dans la mesure où ces intérêts sont également pertinents pour les intérêts de la sécurité nationale[92].

54. Enfin, il convient de noter qu'un critère standard de moindre intrusion/respect de la proportionnalité est présent dans la plupart des pays sur lesquels des informations ont été recueillies. Ce critère exige que l'autorité requérante démontre, entre autres, qu'il n'existait pas d'autres moyens moins intrusifs d'obtenir les informations demandées, et que l'organe d'autorisation estime que le comportement autorisé est proportionné à ce qui est recherché[93].

---

[86] Disponible ici.
[87] Article 8, paragraphe 2, point a), et article 10, paragraphe 2, point a), de la loi sur les services de renseignement et de sécurité.
[88] Article 216 o et p ; ou autres crimes d'activités de renseignement illégales contre des secrets d'État, révélation de secrets d'État, autres activités de renseignement illégales, participation à des associations violentes, influence de services de renseignement étrangers, incitation et recrutement pour la terreur, voyages dans l'intention de semer la terreur, participation et recrutement pour des activités militaires illégales à l'étranger, délits de privation de liberté, traite des êtres humains, production et diffusion de matériel sexualisant des enfants, recel, blanchiment d'argent, violations de la loi sur le contrôle des exportations de produits stratégiques, de technologies, etc, et certaines violations de la loi sur l'immigration.
[89] Article 588 *septies* du code de procédure pénale.
[90] Voir l'article 4 de la loi (2020:62) sur la lecture secrète des données. Section 4 de la loi (2020:62) sur la lecture des données secrètes, qui renvoie au chapitre 27, section 18a, du code de procédure judiciaire.
[91] Voir l'article 6 de la loi (2020:62) sur la lecture secrète des données. Section 6 de la loi (2020:62) sur la lecture des données secrètes, qui renvoie au chapitre 27, section 2 d, du code de procédure judiciaire.
[92] Section 102(5) de la loi sur les pouvoirs d'investigation (Investigatory Powers Act) de 2016.
[93] Par exemple, en Belgique (article *90ter* § 1 du code de procédure pénale) ; au Canada (article 21 § 2(b) de la loi sur le Service canadien du renseignement de sécurité) ; en Suède (article 3 de la loi (2020:62) sur la lecture

2. *Ratione personae*

55. Le **Danemark**[94], la **Finlande**[95], l'**Italie**, les **Pays-Bas**, la **Norvège**[96], l'**Espagne**[97] limitent la possibilité d'utiliser des logiciels espions aux seuls appareils appartenant aux personnes soupçonnées d'avoir commis les infractions prévues par la loi ou à celles qui représentent une menace pour la sécurité nationale ou une menace équivalente, comme le prévoit le cadre juridique national applicable. En **Belgique**[98], **Allemagne**[99], **Suède**[100], **Suisse**[101], et au **Royaume-Uni**[102], des tiers suffisamment liés à la cible principale peuvent également faire l'objet d'une surveillance par logiciel espion.

3. *Ratione temporis*

56. Il ressort de l'analyse comparative que les délais pour l'autorisation de l'utilisation de logiciels espions comme outil de surveillance ciblée sont, dans la plupart des cas examinés, plus courts lorsque les autorisations sont données dans le cadre de procédures pénales que lorsqu'elles le sont dans le cadre d'enquêtes de renseignement.

---

des données secrètes) ; en Suisse (article 27 IntelSA) ; au Royaume-Uni (article 102(1)(b) de la loi de 2016 sur les pouvoirs d'investigation).

[94] Section 791(b) de la loi sur l'administration de la justice.

[95] Article 23 § 3 de la loi sur les mesures coercitives.

[96] Article 216 o § 4 de la loi sur la procédure pénale. En ce qui concerne les enquêtes de renseignement, il convient de préciser que le service de renseignement ne peut recourir à la surveillance ciblée ou à d'autres formes de surveillance de personnes se trouvant en Norvège. Une interdiction explicite figure à l'article 4, paragraphe 1, de la loi sur le service de renseignement de 2020.

[97] Article 588 *septies* (c) du code de procédure pénale.

[98] Article *90-ter* § 1 du code de procédure pénale : une surveillance peut être ordonnée à l'encontre de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.

[99] Conformément à l'article 100b § 3 du code de procédure pénale, lorsqu'il y a lieu de supposer, sur la base de certains faits, que : (i) l'accusé utilise les systèmes de technologie de l'information de l'autre personne ; et (ii) l'interférence avec les systèmes de technologie de l'information de l'accusé ne permettra pas à elle seule d'établir les faits ou de déterminer le lieu où se trouve un coaccusé. Voir également l'article 49 § 3 de la loi sur l'Office fédéral de police criminelle (lorsque cela est inévitable).

[100] Section 4a de la loi (2020:62) sur la lecture des données secrètes.

[101] Dans le cadre d'une procédure pénale, l'article 270 du code de procédure pénale prévoit que, outre l'accusé, des tiers peuvent être surveillés s'il existe des informations spécifiques selon lesquelles : (i) l'accusé utilise l'adresse postale ou le service de télécommunications du tiers, ou (ii) le tiers reçoit certaines communications pour le compte de l'accusé ou transmet des communications de l'accusé à une autre personne. De même, le Service fédéral de renseignement peut ordonner une mesure de recherche d'informations soumise à autorisation à l'égard d'un tiers s'il y a lieu de croire que la personne auprès de laquelle il est envisagé de recueillir des informations utilise des locaux, des véhicules ou des installations de stockage appartenant au tiers ou des adresses postales, des points de connexion de télécommunication, des systèmes informatiques ou des réseaux informatiques de ce dernier pour transmettre, recevoir ou stocker des informations (article 28 de la loi fédérale du 25 septembre 2015 sur le service de renseignement (« LSCR »)). La mesure ne peut être ordonnée si le tiers appartient à l'un des groupes professionnels mentionnés aux articles 171-173 du code de procédure pénale.

[102] Section 101 de l'IPA 2016.

57. Dans les procédures pénales, dans les pays qui utilisent des logiciels espions, les délais vont de 15 jours[103] à six mois[104], avec des délais de quatre semaines[105], d'un mois[106] ou de trois mois[107].

58. Dans les enquêtes de renseignement, ce délai va de quatre semaines[108], à six mois[109], d'autres pays prévoyant des délais d'un mois[110], 40 jours[111], deux mois[112], ou trois mois[113].

D. Autorisation de mesures de surveillance ciblées

59. Dans la mesure où l'autorisation des mesures de surveillance ciblée dans le cadre d'enquêtes/procédures pénales est confiée au pouvoir judiciaire dans l'écrasante majorité des États pour lesquels des données sont disponibles[114], l'approche diffère en ce qui concerne l'autorisation des mesures de surveillance ciblée dans le cadre d'enquêtes de renseignement. En **France**[115], en **Allemagne**[116], au **Luxembourg**[117], aux **Pays-Bas**[118], cette autorisation est

[103] Italie (article 267 § 3 du code de procédure pénale), Norvège (article 216 o § 5 du code de procédure pénale).
[104] Royaume-Uni, article 116 § 2 (b) de la loi sur les pouvoirs d'investigation (Investigatory Powers Act).
[105] Danemark (article 783 de la loi sur l'administration de la justice), Pays-Bas (article 126nba § 3 du code de procédure pénale).
[106] Belgique (article 90 *quater*du code de procédure pénale) ; Finlande (article 24 de la loi sur les mesures coercitives) ; Allemagne (article 100e § 2 du code de procédure pénale - après une période totale de six mois, c'est le tribunal régional supérieur qui décide de toute nouvelle ordonnance de prolongation) ; Luxembourg (article 88-2 § 4 - renouvelable pour une période totale maximale d'un an) ; Espagne (article 588 *septies* (c) du code de procédure pénale - renouvelable pour une période totale maximale de trois mois) ; Suède (article 18 de la loi (2020 :62) sur la lecture de données secrètes - renouvelable ; la loi prévoit également que si les conditions de l'autorisation ont changé, la surveillance doit cesser immédiatement. Les chiffres de 2023 montrent que la période moyenne d'autorisation était de 21 jours, la période médiane étant de 13 jours).
[107] Suisse (article 274 du code de procédure pénale).
[108] Danemark (article 783 de la loi sur l'administration de la justice)
[109] Finlande (article 24 de la loi sur la police et article 33 de la loi sur le renseignement militaire) ; Royaume-Uni (article 116 § 2 (b) de la loi sur les pouvoirs d'investigation).
[110] Suède (article 18 de la loi (2020:62) sur la lecture des données secrètes - renouvelable ; la loi prévoit également que si les conditions de l'autorisation ont changé, la surveillance doit cesser immédiatement. Les chiffres de 2023 montrent que la période moyenne d'autorisation était de 21 jours, la période médiane étant de 13 jours).
[111] Italie (article *4-bis* § 1 de la loi n° 144/2005).
[112] Belgique (article 18/10 § 1).
[113] Allemagne (article 49 § 6(3) de la loi sur l'Office fédéral de police criminelle) ; Luxembourg (article 7 § 1 de la loi SRE), Pays-Bas (article 49 § 4 de la loi sur les services de renseignement et de sécurité de 2017), Espagne (article unique, loi 2/2002 réglementant le contrôle judiciaire préalable du Centre national de renseignement) ; Suisse (article 26 § 6 de la loi IntelSA).
[114] Les exceptions notables sont l'Irlande, Malte et le Royaume-Uni, *voir* respectivement les notes de bas de page 120, 146 et 121 ci-dessous.
[115] Si le Premier ministre décide de ne pas prendre en considération un avis négatif rendu par la *Commission nationale de contrôledes*techniques de *renseignement(*CNCTR), la CNCTR doit immédiatement saisir le Conseil d'État. C'est le Conseil qui prend la décision finale.
[116] En Allemagne, les services de renseignement fédéraux ne sont pas autorisés à procéder à des interceptions de télécommunications à la source tant qu'ils n'ont pas reçu l'ordre du ministère fédéral de l'Intérieur et de la Communauté et que l'opération n'a pas été autorisée par la Commission G10 (commission composée de cinq membres, dont trois au moins doivent être habilités à exercer des fonctions judiciaires, nommés par le groupe parlementaire de contrôle), tandis que le service de renseignement fédéral (BND) doit obtenir l'autorisation du Conseil de contrôle indépendant (Unabhängiger Kontrollrat) avant de pouvoir entreprendre des mesures d'exploitation de réseaux informatiques. Conformément à l'article 23 § 7, de la loi sur le service fédéral de renseignement, le Conseil doit autoriser les recherches de données avant leur utilisation. En cas d'urgence, un membre du Conseil peut autoriser de telles mesures, mais elles doivent être examinées par le Conseil dans les plus brefs délais.
[117] Ordonné par le Comité ministériel du renseignement à la demande écrite du directeur de l'Agence nationale du renseignement et après approbation d'une commission spéciale composée de hauts magistrats, à savoir le président de la Cour supérieure de justice, le président du tribunal administratif et le président du tribunal d'arrondissement de Luxembourg (article 7, paragraphe 4, de la loi SRE).
[118] Le chef de service du Service de renseignement et de sécurité général (AIVD) ou du Service de renseignement et de sécurité militaire (MIVD). Un ministre doit autoriser l'utilisation de ce pouvoir d'investigation en vertu de l'article 45 de la loi sur les services de renseignement et de sécurité. La Commission des pouvoirs d'investigation (TIB) examine en outre la légalité de l'utilisation de ce pouvoir avant qu'il ne soit utilisé.

confiée à l'exécutif avec l'appui d'un organe d'autorisation indépendant. En **Belgique**, une décision motivée du chef du département des services de sécurité est requise, après avis conforme d'une commission administrative spécialisée[119]. En **Irlande**[120] et au **Royaume-Uni**[121], l'exécutif et le judiciaire ont tous deux un rôle à jouer dans la procédure d'autorisation des mesures de surveillance ciblée. En **Bulgarie**, **Bosnie-Herzégovine**[122], **Canada**, **Croatie**[123], **Danemark**, **Estonie**[124], **Finlande**[125], **Grèce**[126], **Islande**, **Italie**[127], **Kosovo**[128], **Kirghizstan**,

[119] La Commission chargée de contrôler les méthodes de collecte de données spécifiques et exceptionnelles des services de renseignement et de sécurité (Commission BIM), composée de trois magistrats et présidée par un juge d'instruction.

[120] Une autorisation judiciaire est requise pour certains types de dispositifs de surveillance (tels que la pose de micros audio ou de caméras vidéo secrètes) en vertu de la loi de 2009 sur la justice pénale (surveillance), tandis qu'une autorisation de l'exécutif (le ministre de la justice) est requise pour l'interception des communications téléphoniques en vertu de la loi de 1993 sur l'interception des paquets postaux et des télécommunications. La loi de 2011 sur les communications (conservation des données), telle que modifiée par la loi de 2022, confère à la Haute Cour le pouvoir de conserver les données de l'annexe 2 (données relatives à la localisation et au trafic des communications). L'accès aux données de source Internet et aux données de l'annexe 2 est accordé par un juge de la District Court. En ce qui concerne les données des utilisateurs, il n'est pas nécessaire d'obtenir l'autorisation d'un juge ou d'un organisme indépendant.

[121] Section 108 de l'Investigatory Powers Act : dans le cadre des enquêtes criminelles et des enquêtes de renseignement, l'Investigatory Powers Commissioner (IPC) approuve les mandats d'interférence des équipements à la demande des autorités publiques, telles que le secrétaire d'État, les agences de renseignement, la police et les autorités locales. L'IPC est assisté par une équipe de commissaires judiciaires. Ceux-ci sont nommés par le Premier ministre et doivent exercer ou avoir exercé de hautes fonctions judiciaires.

[122] Le président de la Cour de Bosnie-Herzégovine ou un juge délégué par lui. Une décision de la Cour constitutionnelle de Bosnie-Herzégovine (U-21/16 du 1er juin 2017) a déclaré inconstitutionnelle la disposition (article 78, paragraphes 3, 4 et 5 de la loi sur l'Agence de renseignement et de sécurité de Bosnie-Herzégovine) qui accordait auparavant au directeur général de l'Agence des services de sécurité la possibilité d'approuver la mesure de renseignement avec le consentement du président du Conseil des ministres de Bosnie-Herzégovine si le retard causait un préjudice irréparable à la sécurité de la Bosnie-Herzégovine. S'appuyant sur la jurisprudence de la CourEDH, la Cour a estimé que la loi ne demandait pas au directeur général d'envoyer une demande écrite au juge et ne précisait pas non plus le délai dans lequel le juge devait approuver ou suspendre l'application de ces mesures.

[123] Un mandat judiciaire de la plus haute juridiction (la Cour suprême de la République de Croatie) est nécessaire pour les mesures plus intrusives suivantes : surveillance secrète du contenu des communications, censure postale (surveillance secrète du courrier et d'autres envois), surveillance secrète et enregistrement technique de l'intérieur des installations, des espaces fermés et des objets, ainsi que surveillance secrète et contrôle, avec enregistrement audio du contenu des communications entre personnes dans des espaces ouverts et publics (article 36 de la loi de 2006 sur le système de sécurité et de renseignement). D'autres mesures moins intrusives, telles que la surveillance secrète des données relatives au trafic des télécommunications, la localisation de l'utilisateur et les télécommunications internationales, la surveillance et le contrôle secrets, avec enregistrement d'images et de photos de personnes dans des espaces ouverts et publics, l'achat secret de documents et d'objets, peuvent être prises si elles sont approuvées par l'un des directeurs des agences de sécurité et de renseignement dans le cadre de leur champ d'activité respectif (article 38).

[124] Le président d'un tribunal administratif ou un juge administratif désigné par lui.

[125] Mais la simple installation et le retrait d'un dispositif ou d'un logiciel ne nécessitent pas l'autorisation d'un tribunal, voir l'article 42 de la loi sur le renseignement militaire et l'article 26 de la loi sur les mesures coercitives.

[126] Conformément à l'article 4 de la loi 5002/2022, l'ordonnance pertinente (διάταξη) est émise par le procureur compétent à la suite d'une demande de l'Agence nationale de renseignement grecque (EYP). Cependant, le procureur compétent est détaché (αποσπασμένος) pour une mission à temps plein auprès de l'EYP (en vertu de l'article 5§3 de la loi 3649/2008) et son indépendance est donc souvent contestée. L'ordonnance du procureur du PEJ doit être confirmée par un second procureur (de haut rang) qui sert soit à la Cour d'appel, soit à la Cour suprême (Areios Pagos).

[127] L'article 4 du décret-loi n° 144 du 27 juillet 2005 confère au président du Conseil des ministres le pouvoir d'autoriser les directeurs des services de renseignement de sécurité visés à l'article 2, paragraphe 2, de la loi n° 124 du 3 août 2007 à demander l'autorisation d'intercepter des communications ou des conversations, y compris par des moyens télématiques, ainsi que d'intercepter des communications ou des conversations, même dans les lieux visés à l'article 614 du Code pénal. 124 du 3 août 2007 à demander l'autorisation d'intercepter des communications ou des conversations, y compris par voie télématique, ainsi que d'intercepter des communications ou des conversations, même dans les lieux visés à l'article 614 du code pénal, si cela est jugé nécessaire à l'exécution des tâches qui leur sont confiées par les articles 6 et 7 de la loi n° 124 du 3 août 2007. L'autorisation est demandée au Procureur Général près la Cour d'Appel de Rome, qui l'accorde si les conditions prévues à l'article 4-bis sont remplies.

[128] Un juge de la Cour suprême à la demande du directeur ou du directeur adjoint de l'Agence de renseignement du Kosovo (KIA), *voir la* loi n° 03/L-063 sur l'Agence de renseignement du Kosovo.

Lituanie[129], **République de Moldova**[130], **Monaco**, **Macédoine du Nord**[131], **Norvège**[132], **Portugal**[133], **Roumanie**, **Serbie**[134], **République slovaque**[135], **Espagne**[136], **Suède**[137], **Ukraine**[138], **États-Unis**[139] le pouvoir d'autorisation est confié au pouvoir judiciaire. En **Corée**, les mesures de surveillance ciblée dans le cadre d'enquêtes de renseignement nécessitent soit l'autorisation du président de la Haute Cour, soit l'approbation du président de la République[140]. En **Pologne**, le pouvoir d'autorisation est normalement confié au pouvoir judiciaire[141], mais en ce qui concerne la surveillance secrète de ressortissants étrangers, un régime spécial permet aux autorités de procéder à une surveillance secrète pendant trois mois sans autorisation judiciaire préalable[142]. En **Suisse**, la situation est différente selon que la cible se trouve en Suisse ou à l'étranger. Dans le premier cas, le pouvoir judiciaire et le pouvoir exécutif sont impliqués[143].

[129] Article 10 de la loi sur le renseignement criminel.

[130] *Avec la réserve* que la fouille d'objets et de documents, la surveillance visuelle et la collecte d'informations peuvent être ordonnées avec l'autorisation du chef de la subdivision spécialisée des services de sécurité, cfr. l'article 27 en conjonction avec l'article 20 de la loi n° 59/2012 sur l'activité d'enquête spéciale.

[131] Un juge de la Cour suprême à la demande du procureur général de la République de Macédoine du Nord, à l'initiative du ministre de l'intérieur ou du ministre de la défense (article 20 de la loi sur la surveillance des communications).

[132] Les décisions relatives à la collecte d'informations électroniques transfrontalières (trafic Internet) doivent être approuvées par un tribunal (voir l'article 8-1 de la loi sur le renseignement de 2020).

[133] Une formation de trois juges des chambres pénales de la Cour suprême de justice.

[134] Conformément à la loi sur l'agence d'information sur la sécurité (article 15), la décision sur la proposition motivée du directeur de l'agence est prise par le président de la Cour supérieure de Belgrade, c'est-à-dire un juge qu'il délègue parmi les juges du département spécial de cette Cour, qui, conformément à la loi, traite les affaires relatives aux infractions pénales liées au crime organisé, à la corruption et à d'autres infractions pénales particulièrement graves.

[135] En vertu de l'article 4a de la loi sur la protection contre l'interception (PAIA), la juridiction compétente est le tribunal régional dans le district duquel se trouve l'autorité publique requérante. La seule exception concerne les crimes relevant de la compétence du Tribunal pénal spécialisé.

[136] Le Conseil général du pouvoir judiciaire nomme un magistrat de la Cour suprême (de la chambre administrative ou pénale) et un suppléant pour autoriser les interceptions de communications par les services de renseignement. Tous deux doivent avoir au moins trois ans d'ancienneté à la Cour suprême. Leur mandat est de cinq ans. Ce juge peut autoriser
l'interception des communications sur proposition du directeur du CNI. Le 8 septembre 2023, le groupe parlementaire du Parti nationaliste basque a présenté un projet de loi visant à modifier la loi 11/2002 et la loi organique 2/2002. Le projet de loi propose un renforcement du contrôle judiciaire préalable en remplaçant la figure du magistrat unique de la Cour suprême chargé de ces questions par une chambre de trois magistrats de la Cour suprême. Le projet de loi a été adopté en tant qu'initiative complète par le Congrès le 27 février 2024, mais n'a pas encore été adopté par le Sénat.

[137] Article 14 de la loi (2020:62) sur la lecture des données secrètes.

[138] L'article 15 § 2 de la loi n° 912-IX sur le renseignement prévoit qu'une agence de renseignement peut commencer à mener des activités de renseignement uniquement surla base d'une décision de justice. Sur décision du chef de l'agence de renseignement, une mesure de renseignement peut être prolongée jusqu'à l'obtention d'une décision de justice, mais pas plus de 72 heures à partir du moment de l'identification de la personne.

[139] Un tribunal spécialisé (le United States Foreign Intelligence Surveillance Court), sert d'organe d'approbation pour l'utilisation des outils de surveillance. La collecte de communications électroniques de non-américains situés en dehors des États-Unis ne nécessite pas de mandat.

[140] L'approbation présidentielle n'est requise que dans des circonstances particulières, tandis que l'autorisation judiciaire est la procédure normale.

[141] La demande de contrôle opérationnel est soumise au tribunal de district (*sąd okręgowy*) compétent, accompagnée des documents justifiant la nécessité de sa mise en œuvre. Les demandes d'autorisation de surveillance sont examinées par des juges uniques et, conformément à l'article 47a de la loi sur le système des tribunaux communs (*Ustawa o ustroju sądów powszechnych*), elles sont confiées à un juge de garde. Un procureur et un représentant de l'autorité demandant le contrôle opérationnel peuvent participer à la réunion.

[142] Article 9 § 1 de la loi antiterroriste ; *voir Pietrzak et Bychawska-Siniarska et autres c. Pologne*, précité, §§ 53-54.

[143] La mesure de renseignement doit être autorisée par le président d'une section spéciale de la Cour administrative fédérale (article 29 IntelSA). En outre, la mesure doit être autorisée par le ministre de la défense après consultation du ministre des affaires étrangères et du ministre de la justice. Le Conseil fédéral doit être informé des cas d'une importance particulière (article 30 IntelSA).

Dans le second cas, aucune autorisation judiciaire n'est requise[144]. En **Hongrie**[145] et à **Malte**[146], le pouvoir d'autoriser des mesures de surveillance ciblée dans le cadre d'enquêtes de renseignement est confié à l'exécutif.

60. Dans de nombreux États, les services répressifs ou les services de renseignement ont la possibilité, dans des cas exceptionnels et urgents (par exemple, en cas de danger pour la vie humaine, la santé, la sécurité publique ou la sûreté de l'État), de procéder à une surveillance ciblée en l'absence d'autorisation préalable, à condition que cette autorisation soit accordée par l'organe compétent dans un délai qui varie entre 24 heures[147], deux jours[148], trois jours[149] et cinq jours[150].

E. Mécanismes de contrôle

61. Les données dont dispose la Commission de Venise montrent que les systèmes nationaux de contrôle sont diversifiés en termes de cadre juridique, d'organisation, de composition, de mandat, de fonctions et de pouvoirs. Un large éventail d'acteurs différents semble être impliqué dans les systèmes nationaux de contrôle, notamment le pouvoir judiciaire (cours ou tribunaux ou organes judiciaires similaires), les parlements ((sous-)commissions parlementaires spécialisées), les institutions nationales indépendantes (par exemple, les médiateurs) et les agences de contrôle spécialisées (dotées d'un mandat de contrôle spécial) qui ne font pas partie du parlement, de l'exécutif ou des agences qu'elles contrôlent[151].

62. Le contrôle des mesures de surveillance ciblée ordonnées dans le cadre d'une procédure pénale est normalement confié au pouvoir judiciaire dans le cadre du contrôle général de la procédure en cours[152].

---

[144] Seul le Conseil fédéral est habilité à décider des attaques contre les réseaux informatiques (article 37 § 1, IntelSA). En cas d'exploitation de réseaux informatiques (§ 2), c'est le ministre de la Défense, après consultation des ministres des Affaires étrangères et de la Justice.

[145] Selon la loi sur la sécurité nationale, c'est le ministre de la justice qui est chargé de fournir cette autorisation.

[146] En vertu du chapitre 391 de la loi sur le service de sécurité, le service de sécurité de Malte peut obtenir l'autorisation d'intercepter ou d'interférer avec des communications au moyen d'un mandat délivré par le ministre responsable du service de sécurité, c'est-à-dire, en règle générale, le ministre de l'intérieur. La loi s'applique également aux procédures pénales.

[147] Croatie (article 36 § 2 de la loi sur le système de sécurité et de renseignement de la République de Croatie) ; Danemark (article 783 de la loi sur l'administration de la justice) ; Estonie (article 126^4 § 2 et § 3 du code de procédure pénale) ; Finlande (article 24 de la loi sur les mesures coercitives, article 24 de la loi sur la police et article 33 de la loi sur le renseignement militaire) ; République slovaque, article 114 § 2 de la loi sur l'administration de la justice (PAIA).

[148] Italie (article 267 du code de procédure pénale) ; Kosovo (loi n° 03/L-063 sur l'Agence de renseignement du Kosovo), Roumanie (article 141 § 1 du code de procédure pénale), Saint-Marin (article 4 de la loi n° 98 du 21 juillet 2009 (« loi sur les interceptions »)).

[149] Kosovo (dans le cadre de procédures pénales - article 90 § 2 du code de procédure pénale) ; Ukraine (article 15 de la loi « sur le renseignement ») ; Royaume-Uni (article 109 § 3 de l'IPA 2016).

[150] Pologne, article 19 § 3 de la loi sur la police.

[151] Une vue d'ensemble des mécanismes de contrôle en place dans les pays de l'UE dans le contexte de la surveillance par les services de renseignement se trouve dans le rapport de la FRA, cité ci-dessus. *Voir également* Conseil de l'Europe, Commissaire aux droits de l'homme, *La surveillance démocratique et effective des services de sécurité nationale*, mai 2015.

[152] Quelques exceptions notables : aux Pays-Bas, outre le contrôle judiciaire pendant le procès, l'autorité d'inspection du ministère de la justice et de la sécurité a pour mandat spécial de vérifier (principalement les procédures) l'utilisation du piratage informatique comme moyen d'investigation. Elle présente un rapport annuel mais n'a pas de pouvoirs contraignants pour remédier à la situation. En Norvège, l'article 216 h de la loi de procédure pénale de 1981 exige la création d'un organe indépendant chargé de contrôler la légalité de l'utilisation et du stockage des mesures de contrôle des communications (écoutes téléphoniques, surveillance, écoutes de données). Cet organe, composé d'au moins 3 membres (actuellement 6 membres), est nommé par le gouvernement. Le président doit remplir les conditions requises pour être juge à la Cour suprême. L'organe peut traiter toute question soulevée par des particuliers ou des organisations concernant la surveillance policière. L'organe peut également, de sa propre initiative, traiter toute question et doit donner la priorité aux questions qui ont fait l'objet d'un débat public ou d'une critique. L'organe a accès à toutes les informations relatives aux mesures de contrôle des communications, y compris les écoutes téléphoniques, les vidéos, les écoutes de données, etc.

63. En ce qui concerne le contrôle des mesures de surveillance mises en œuvre par les agences de renseignement, la Commission de Venise a observé que des organes d'experts indépendants effectuent ce contrôle dans un certain nombre de pays, notamment en **Autriche**[153], **Belgique**[154],

En Suède, outre le contrôle judiciaire, la Commission sur la sécurité et la protection de l'intégrité (voir la loi sur la supervision de certaines activités de lutte contre la criminalité 2007:980) a pour mandat de veiller à ce que : les activités de surveillance de la police, y compris la police de sécurité, et l'archivage des données personnelles par cette dernière, soient menées conformément aux lois et autres réglementations. Il s'agit d'un organe de 10 membres nommés par le gouvernement pour une période renouvelable de quatre ans maximum. Tous les partis représentés au Riksdag peuvent proposer un membre de la Commission. La plupart des partis ont nommé des hommes politiques expérimentés, dont certains sont des députés en activité. Le président et le vice-président doivent être ou avoir été des juges titulaires ou avoir une expérience juridique équivalente. L'article 2 de la loi sur la surveillance prévoit que la SIN exerce sa surveillance par le biais d'inspections et d'autres enquêtes. Elle se saisit chaque année d'un certain nombre d'affaires de sa propre initiative. La SIN présente un rapport annuel au gouvernement. Une disposition importante est celle selon laquelle, contrairement à d'autres mesures d'investigation secrètes, telles que l'interception des télécommunications, dans les cas de lecture secrète de données, le tribunal qui délivre l'autorisation a l'obligation d'informer la SIN lorsqu'une autorisation a été accordée (article 21 de la loi sur la lecture secrète de données). Cette obligation proactive permet au SIN d'avoir une meilleure vue d'ensemble de la manière dont la loi est appliquée et de décider s'il convient ou non d'ouvrir une enquête de contrôle. Au Royaume-Uni, l'Investigatory Powers Tribunal (IPT) est un tribunal entièrement indépendant chargé d'examiner les plaintes relatives à l'utilisation abusive des pouvoirs d'investigation. Il est composé de personnes ayant exercé de hautes fonctions judiciaires (et le président doit être une telle personne) et d'avocats chevronnés. Le Tribunal a également le pouvoir d'accorder des compensations et peut ordonner la destruction d'informations et de dossiers d'informations ainsi que l'annulation de mandats.

[153] Le délégué à la protection juridique est responsable du contrôle des traitements de données visés à l'article 12, paragraphes 1 et 1a, de la loi sur la sécurité de l'État et le renseignement, ainsi que de la protection juridique visée à l'article 6, paragraphes 1 et 2, de la loi. Les unités organisationnelles compétentes doivent obtenir son autorisation préalable avant d'effectuer les tâches visées à l'article 6, paragraphes 1 et 2, de la loi. Il doit avoir accès à tous les documents, enregistrements et données traitées nécessaires, ainsi qu'à tous les locaux dans les conditions prévues par la loi. Il peut également déposer une plainte auprès de l'autorité chargée de la protection des données au nom des personnes concernées. Chaque année, le délégué à la protection juridique rend compte au ministre de l'intérieur de ses activités et de ses perceptions dans le cadre de l'exercice de ses fonctions (article 15, paragraphe 4, de la loi). La direction fait également rapport au ministre de l'intérieur et publie un rapport annuel sur les développements actuels et possibles en matière de protection de la constitution afin d'informer le public. La Commission de contrôle indépendante pour la protection de la Constitution est chargée de contrôler les activités des unités organisationnelles et d'enquêter sur les allégations concernant les activités des unités organisationnelles. La Commission a accès à tous les locaux et peut inspecter les documents et les dossiers. Elle soumet un rapport annuel au ministre fédéral de l'intérieur et à la sous-commission permanente de la commission des affaires intérieures (du Conseil national) et prépare un rapport annuel informant le public de ses activités. Elle peut à tout moment adresser des recommandations au ministre fédéral de l'intérieur.

[154] Le Comité permanent R est chargé de contrôler le fonctionnement général des services de renseignement et de sécurité. Il s'agit d'un organe collégial : il est composé de trois membres dont un président qui doit être un magistrat. Il contrôle la légalité des décisions relatives aux méthodes spécifiques et exceptionnelles, ainsi que le respect des principes de proportionnalité et de subsidiarité. Lorsque le Comité permanent R constate l'illégalité d'une méthode ou le non-respect du principe de proportionnalité ou de subsidiarité, il peut mettre fin à la méthode. Toutes les informations recueillies à l'aide de la méthode doivent alors être détruites.

Bulgarie[155], **Canada**[156], **Croatie**[157], **Danemark**[158], **Finlande**[159], **France**[160], **Allemagne**[161], **Grèce**[162], **Lituanie**[163], **Pays-Bas**[164], **Macédoine du Nord**[165], **Portugal**[166], **Suède**[167]. En **Suisse**,

[155] Le Bureau national de contrôle des moyens de renseignement spéciaux.
[156] L'Agence de surveillance de la sécurité nationale et du renseignement (ASNR) est un organe de contrôle indépendant et externe qui rend compte au Parlement. Le NSIRA est habilité à examiner les activités du gouvernement du Canada en matière de sécurité nationale et de renseignement afin de s'assurer qu'elles sont légales, raisonnables et nécessaires. À l'issue d'un examen, le NSIRA peut formuler des conclusions ou des recommandations qu'il juge appropriées. Le NSIRA enquête également sur les plaintes du public concernant les principales agences et activités de sécurité nationale, ainsi que sur les plaintes relatives aux habilitations de sécurité. À la suite d'une enquête, la NSIRA doit fournir un rapport contenant les conclusions de l'enquête et toute recommandation qu'elle juge appropriée. Les conclusions et les recommandations formulées par la NSIRA ne sont pas contraignantes.
[157] Le Conseil pour le contrôle civique des agences de renseignement de sécurité effectue un contrôle ex-post régulier des agences, axé sur la légalité du travail et la mise en œuvre de mesures spéciales de collecte de données. Il agit sur la base de demandes envoyées par des citoyens et des personnes morales concernant des irrégularités potentielles et des violations des droits humains. Le Conseil est composé de sept citoyens nommés par le Parlement sur la base d'un appel public pour des mandats de quatre ans, mais disposant d'une expertise spécifique et d'une habilitation de sécurité complète. Lorsque, dans le cadre du contrôle effectué, il est établi qu'il y a eu des actes illégaux, le président du Conseil en informe le président de la République, le président du Parlement, le président du gouvernement et le procureur général de l'État.
[158] Le Conseil danois de surveillance du renseignement a le pouvoir d'accéder à toutes les données collectées par les services de sécurité.
[159] Le médiateur du renseignement supervise les autorités civiles et militaires chargées du renseignement : le Service finlandais de sécurité et de renseignement, la Division du renseignement du Commandement de la défense et l'Agence de renseignement de la défense finlandaise. Conformément à l'article 15 de la loi sur le contrôle de la collecte de renseignements, le médiateur du renseignement est habilité à ordonner la suspension ou l'arrêt de l'utilisation de la méthode de renseignement s'il estime que l'autorité de renseignement a agi de manière illégale dans la collecte de renseignements.
[160] La CNCTR veille à ce que la collecte de renseignements se fasse dans le respect du Code de la sécurité intérieure. Selon l'article L831-1 du Code, la CNCTR est composée de quatre parlementaires (deux députés et deux sénateurs), deux membres du Conseil d'État, deux magistrats, un expert en techniques de communication électronique. La Commission peut émettre des avis sur la mise en œuvre des techniques de recueil de renseignements, mais ceux-ci ne sont pas contraignants.
[161] La Commission du G10 et le Conseil de surveillance indépendant. Le premier est constitué par le Parlement conformément à l'article 10 § 2 de la Grundgesetz allemande et est limité aux mesures concernant les télécommunications. Il remplace le contrôle exercé par le pouvoir judiciaire. Le deuxième agit en tant qu'organe de contrôle administratif. Ses membres sont six juges de la Cour suprême fédérale et/ou de la Cour administrative fédérale, qui sont élus par le groupe parlementaire de contrôle pour 12 ans.
[162] L'Autorité hellénique pour la sécurité des communications et la protection de la vie privée (ADAE). Conformément à l'article 6 de la loi n° 3115/2003, l'ADAE est habilitée à effectuer des audits des installations, des équipements, des archives, des bases de données et des documents du PEJ.
[163] Le médiateur du renseignement, créé en 2022, est autorisé à enquêter sur les cas où il existe des signes que les institutions ou les agents du renseignement abusent de leurs pouvoirs, portent atteinte aux droits humains et aux libertés, compromettent les intérêts légitimes ou enfreignent les réglementations relatives au traitement des données à caractère personnel à des fins de sécurité nationale ou de défense.
[164] Le Comité néerlandais de surveillance des services de renseignement et de sécurité (CTIVD) est l'organe de contrôle des services de renseignement et de sécurité. Le CTIVD effectue un contrôle lors de l'application du piratage informatique en tant que pouvoir d'investigation, c'est-à-dire qu'il vérifie les risques techniques encourus et les dispositifs ciblés. Il publie également des rapports sur la légalité du piratage informatique en tant que pouvoir d'investigation. Cependant, dans le cadre d'une nouvelle législation relative aux « acteurs étatiques dotés de programmes cybernétiques » en 2024, le CTIVD dispose de pouvoirs contraignants limités dans son contrôle des pouvoirs de piratage informatique. En vertu de cette nouvelle législation, les services de renseignement et de sécurité peuvent faire appel d'une décision du TIB et du CTIVD, et un juge peut statuer sur cette question. Aucun jugement n'a encore été rendu. Les personnes qui estiment avoir été traitées de manière illégale ou injuste par les services de renseignement et de sécurité peuvent déposer une plainte auprès du ministre de l'intérieur et des relations au sein du royaume ou du ministre de la défense. Si elles ne sont pas satisfaites de la manière dont leur plainte a été traitée, elles peuvent déposer une plainte auprès du CTIVD. Le service des plaintes peut rendre des décisions contraignantes après un comportement illégal des services de renseignement et de sécurité.
[165] Le Conseil pour le contrôle civil est établi pour assurer le contrôle civil des mesures de surveillance des communications. Nommé par l'Assemblée de la République de Macédoine du Nord, le Conseil est composé d'un président et de six membres, dont le mandat est de trois ans et n'est pas renouvelable. Parmi les membres figurent trois experts et trois représentants d'organisations non gouvernementales spécialisées dans les droits humains, la sécurité et la défense. Le Conseil présente un rapport annuel sur ses activités à l'Assemblée avant la fin du mois de février de chaque année. Le Conseil peut agir de sa propre initiative ou en réponse à des plaintes de citoyens.

outre la surveillance par un organe d'experts[168], l'autosurveillance et le contrôle et la surveillance par l'exécutif[169] existent également. Au **Royaume-Uni**, le régime de surveillance comprend à la fois des organes d'experts et le pouvoir judiciaire[170]. Aux **États-Unis**, l'exécutif et le judiciaire sont tous deux impliqués[171]. En **Irlande**[172], un contrôle judiciaire indépendant de l'application des lois pertinentes est effectué par un juge de la Haute Cour en exercice, désigné à cet effet[173]. Au **Kirghizstan**[174] et en **République de Moldova**[175], le contrôle de l'application des lois par les organismes menant des activités de renseignement est confié au ministère public. A **Malte**[176],

[166] Le Conseil de surveillance du système de renseignement de la République portugaise contrôle et supervise l'activité du secrétaire général du système de renseignement et des services de renseignement, en veillant au respect de la Constitution et de la loi, avec un accent particulier sur la préservation des droits, des libertés et des garanties. Il est composé de trois citoyens éminents, indépendants, élus par l'Assemblée de la République, à la majorité des 2/3, pour un mandat de quatre ans ; cet organe, entre autres compétences, supervise la procédure d'accès aux données de télécommunications et d'Internet et aux données ainsi obtenues par les services de renseignement. La loi sur le système d'information de la République portugaise établit également une commission de surveillance des données, composée de trois magistrats du bureau du procureur général, nommés et habilités par le procureur général de la République. La Commission de contrôle des données est l'autorité publique compétente pour contrôler le respect des principes et la conformité aux règles relatives à la qualité et à la sauvegarde de la confidentialité et de la sécurité des données obtenues conformément à la procédure obligatoire et légalement liée prévue par la loi organique nº 4/2017.

[167] *Voir* note de bas de page 152 ci-dessus.

[168] L'autorité indépendante de surveillance supervise les activités de renseignement du SRC, des autorités cantonales d'exécution et d'autres entités et tiers mandatés par le SRC, et contrôle ces activités du point de vue de leur légalité, de leur opportunité et de leur efficacité. Elle a accès à toutes les informations et à tous les documents pertinents, ainsi qu'à tous les locaux utilisés par les entités soumises à la surveillance. Cf. articles 76-78 de l'IntelSA.

[169] Cfr. Article 80 de l'IntelSA.

[170] La CIP procède à un audit détaillé et établit des rapports sur l'utilisation des pouvoirs d'enquête, tandis que le TPI examine les plaintes relatives à l'utilisation abusive des pouvoirs d'enquête (*voir la* note de bas de page 152 ci-dessus).

[171] Le Conseil de surveillance de la vie privée et des libertés civiles (PCLOB) est chargé d'examiner les nouvelles politiques et procédures mises en œuvre par les agences de renseignement et procède à un examen annuel de la procédure de recours de la Cour de contrôle de la protection des données, tandis que la FISC et la Cour de contrôle de la protection des données (DPRC) sont chargées d'assurer la surveillance. Le DPRC offre un mécanisme de recours par le biais d'un examen indépendant et impartial des plaintes spécifiques déposées par des personnes qui allèguent des violations du droit américain dans le cadre des activités de renseignement des États-Unis. Ses décisions sont contraignantes.

[172] L'Irlande ne dispose pas d'une agence de renseignement distincte. Les fonctions de renseignement et de sécurité de l'État relèvent de la responsabilité d'An Garda Síochána et des forces de défense.

[173] Le juge désigné est chargé de surveiller le fonctionnement de la législation et de publier des rapports annuels en vertu de l'article 8 de la loi de 1993, de l'article 12 de la loi de 2009 et de l'article 12 de la loi de 2011. En pratique, cela consiste en des réunions annuelles avec des fonctionnaires du ministère de la Justice, de la police et d'autres agences irlandaises qui utilisent les pouvoirs d'interception et de conservation des données, ainsi qu'en une certaine inspection de leurs dossiers. Le rôle de supervision est une fonction à temps partiel d'un juge. Elle ne bénéficie d'aucun soutien juridique ou technique spécialisé, ce qui signifie qu'il n'y a pas de mémoire institutionnelle et qu'elle dépend du soutien des entités contrôlées. Lorsque le Policing, Security and Community Safety Act 2024 entrera en vigueur, la surveillance primaire sera confiée à un examinateur indépendant.

[174] À la demande du procureur habilité, en rapport avec les documents, les informations et les appels de citoyens reçus par le bureau du procureur concernant des violations des lois lors de la conduite des activités de recherche opérationnelle, ainsi que lors de la vérification de la procédure établie pour la conduite des activités de recherche opérationnelle et de la légalité des décisions prises à cet égard, les chefs de l'organe menant les activités de recherche opérationnelle soumettent audit procureur les documents du service opérationnel qui ont servi de base à la conduite de ces activités.

[175] Article 39 de la loi 59/2012 : le contrôle de l'exécution de la loi est effectué par les procureurs hiérarchiquement supérieurs sur la base des plaintes déposées par les personnes dont les droits et les intérêts légitimes auraient été violés du fait de l'activité d'enquête spéciale ou d'office. Les procureurs hiérarchiquement supérieurs qui effectuent le contrôle ont le droit d'accéder aux informations constituant un secret d'État selon les modalités prévues par la loi.

[176] Le commissaire aux services de sécurité.

en **Pologne**[177] et en **Serbie**[178], c'est l'exécutif qui est impliqué dans le contrôle des activités des agences de renseignement.

64. Un système de contrôle parlementaire des activités des agences de renseignement par le biais de commissions parlementaires spécialisées existe en **Autriche**, en **Belgique**, en **Bosnie-Herzégovine**, en **Bulgarie**, au **Canada**[179], en **Croatie**[180], au **Danemark**, en **Estonie**, en **Finlande**[181], en **France**, en **Allemagne**, **Grèce**, **Italie**[182], **Kosovo**[183], **Kirghizstan**, **Lituanie**, **Luxembourg**[184], **République de Moldova**, **Pays-Bas**, **Macédoine du Nord**[185], **Norvège**[186],

[177] Le ministre de l'intérieur et de l'administration supervise les activités non seulement de la police, mais aussi de certaines forces spéciales, telles que l'agence de sécurité intérieure (ABW). Ce contrôle exécutif consiste notamment à définir des orientations stratégiques et à veiller à ce que les services de sécurité agissent dans le respect de la loi. Toutefois, le rôle du ministre est plus administratif et moins axé sur le contrôle opérationnel quotidien. Le ministre de la justice joue un rôle dans la supervision des activités de surveillance, en particulier celles qui sont liées à des enquêtes criminelles importantes.

[178] Le ministère de l'intérieur et le ministère de la défense supervisent les différents services de sécurité. Ces ministères ont des responsabilités de contrôle administratif et opérationnel.

[179] Le National Security and Intelligence Committee of Parliamentarians (NSICOP) est un comité de parlementaires dont le mandat est très large. Il est notamment chargé d'examiner toute activité menée par un ministère en rapport avec la sécurité nationale ou le renseignement, à moins qu'il ne s'agisse d'une opération en cours et que le ministre compétent estime que cet examen porterait atteinte à la sécurité nationale. La NSICOP soumet un rapport annuel au Premier ministre (qui est ensuite présenté au Parlement), qui comprend les conclusions et les recommandations (non contraignantes) formulées au cours de l'année précédente.

[180] La commission des affaires intérieures et de la sécurité nationale est habilitée à effectuer un contrôle direct sur place de l'agence de sécurité et de renseignement et de l'agence militaire de sécurité et de renseignement. Pour le reste, son travail est basé sur la réception, l'examen et la discussion des rapports des agences (rapports annuels et rapports concernant des cas ou des thèmes spécifiques). Le président de la commission doit être issu des rangs du plus grand parti d'opposition. La commission émet des décisions, des conclusions et des recommandations non contraignantes.

[181] Le comité de surveillance des services de renseignement veille à la bonne mise en œuvre et à l'adéquation des opérations de renseignement, contrôle et évalue les domaines d'intervention des services de renseignement, contrôle et promeut l'exercice effectif des droits fondamentaux et des droits humains dans le cadre des opérations de renseignement, prépare les rapports du médiateur des services de renseignement et traite les conclusions du médiateur des services de renseignement en matière de contrôle.

[182] Article 31 de la loi n° 124/2007 : la commission parlementaire peut obtenir, même en dérogation à l'interdiction établie par l'article 329 du code de procédure pénale, des copies d'actes et de documents relatifs à des procédures et à des enquêtes en cours auprès de l'autorité judiciaire ou d'autres organes d'enquête, ainsi que des copies d'actes et de documents relatifs à des enquêtes et à des investigations parlementaires.

[183] Ses responsabilités comprennent, entre autres, le contrôle de la légalité du travail de l'Agence de renseignement, l'examen des rapports du directeur de l'Agence de renseignement concernant les opérations de l'Agence et des rapports de l'inspecteur général, ainsi que la conduite d'enquêtes concernant le travail de l'Agence.

[184] Chapitre 6 de la loi SRE. La commission parlementaire de contrôle est informée *d'office* tous les six mois des mesures de surveillance et de contrôle des communications ordonnées par le comité ministériel de renseignement à la demande de l'agence de renseignement de l'État. La commission parlementaire de contrôle peut également effectuer des contrôles sur des cas spécifiques.

[185] La Commission de surveillance des mesures de contrôle des communications, présidée par un représentant du principal parti d'opposition, fait également appel à des experts techniques nationaux et internationaux, dont deux sont nommés à titre permanent. L'objectif principal de la Commission est de vérifier que les mesures de surveillance des communications sont mises en œuvre de manière légale et efficace. La Commission examine également le rapport annuel du Procureur général sur les mesures d'enquête spéciales afin d'évaluer l'efficacité de ces mesures. Le contrôle a lieu au moins tous les trois mois, souvent sans préavis. Après chaque session de contrôle, la Commission prépare un rapport détaillé indiquant si le comportement observé était légal ou si des abus ont été détectés. En cas d'irrégularités ou d'abus, la Commission est tenue d'en informer rapidement le procureur général et les autorités compétentes. Enfin, la Commission soumet un rapport annuel à l'Assemblée avant la fin du mois de février de chaque année.

[186] La commission parlementaire norvégienne de contrôle des services de renseignement et de sécurité (commission EOS) a un accès complet à toutes les informations détenues par les services de renseignement, quelle que soit leur classification. La commission EOS peut traiter des plaintes déposées par des particuliers et des dénonciateurs, mais elle peut également enquêter sur des questions de sa propre initiative. Si, au cours d'un contrôle, le comité EOS constate que la surveillance est illégale, il peut exiger la cessation de la surveillance et la suppression de toutes les informations en déposant une requête auprès du tribunal de la ville d'Oslo (voir l'article 7-12 de la loi sur le renseignement de 2020). Il rend compte chaque année au Parlement.

Pologne[187], **Roumanie**, **Serbie**[188], **République slovaque**[189], **Espagne**[190], **Suède**, **Suisse**[191], **Ukraine**[192], **Royaume-Uni**, **États-Unis**[193]. La frontière entre les organes de contrôle parlementaires et les organes de contrôle indépendants/experts n'est pas rigide, puisqu'il existe des organes « hybrides » (voir également le paragraphe 117 ci-dessous).

65. À **Chypre** et au **Portugal**, des commissions parlementaires non spécialisées participent au contrôle des activités des agences de renseignement.

F. Notification des mesures de surveillance ciblées

66. Enfin, la Commission de Venise a analysé l'existence d'un mécanisme de notification post-surveillance dans le cadre de l'exécution de mesures de surveillance ciblée. Dans le cadre des procédures pénales, l'existence d'un mécanisme de notification des mesures de surveillance ciblée a été signalée par la **Bosnie-Herzégovine**[194], **Canada**[195], **Danemark**[196], **Estonie**[197],

[187] La commission des services spéciaux, qui contrôle et examine les opérations menées par l'agence de sécurité intérieure (ABW) et l'agence de renseignement (AW). Cette commission organise des auditions, examine des rapports et veille à ce que les activités des services de sécurité soient menées dans le respect de la loi et des principes démocratiques.
[188] La Commission de contrôle des services spéciaux de sécurité contrôle notamment la constitutionnalité et la légalité du travail des services de sécurité et la légalité de l'application des procédures et mesures spéciales pour la collecte secrète de données.
[189] La Commission spéciale pour le contrôle de l'utilisation des dispositifs informatiques (la Commission n'a toujours pas été mise en place dans la pratique, principalement en raison de désaccords politiques) est composée de huit membres, le président devant appartenir à l'opposition. Elle effectue des inspections au moins une fois par an, mais peut le faire à tout moment de sa propre initiative et sur plainte de toute personne affirmant avoir été soumise à une surveillance illégale. Les pouvoirs de la Commission sont essentiellement des pouvoirs de contrôle. Ses membres ont le droit de pénétrer dans les locaux, d'accéder aux registres et d'obtenir des informations, même classifiées, auprès des autorités compétentes de l'État. Les protocoles des inspections effectuées sont ensuite soumis aux commissions parlementaires compétentes. Si les commissions parlementaires respectives soupçonnent qu'une surveillance a été effectuée en violation de la loi, elles doivent en informer le président du parlement, qui informe alors le procureur général. Deux fois par an, le Parlement doit examiner en séance plénière les rapports des commissions sur l'état de l'utilisation des mesures de surveillance.
[190] La « Commission des secrets officiels » se réunit à huis clos et ses membres sont soumis à une obligation de confidentialité.
[191] La « délégation de contrôle » et la « délégation financière » ont un accès complet et sans entrave à toutes les informations dont elles ont besoin pour s'acquitter de leurs responsabilités en matière de contrôle.
[192] Voir l'article 53 de la loi ukrainienne sur le renseignement. Article 53 de la loi ukrainienne sur le renseignement.
[193] Le House Permanent Select Committee on Intelligence (HPSCI) et le Senate Select Committee on Intelligence (SSCI) assurent le contrôle par le Congrès des activités de renseignement, y compris des pratiques de surveillance. Le HPSCI a des responsabilités législatives et de contrôle sur les programmes, les politiques, les budgets et les opérations de la communauté du renseignement, sur toutes les actions secrètes et sur la collecte, l'exploitation et la diffusion du renseignement humain. Le SSCI assure le contrôle législatif des activités de renseignement du gouvernement américain. Pour ce faire, il organise notamment des auditions avec les hauts responsables des agences de renseignement, mène des enquêtes et examine les programmes de renseignement, et examine et recueille les activités/analyses de renseignement.
[194] Article 119 du code de procédure pénale, avec la possibilité de demander au tribunal l'examen de la légalité de l'ordonnance et de la manière dont la mesure a été mise en œuvre.
[195] Les articles 196 et 196.1 du code pénal prévoient l'obligation d'informer par écrit, après coup, les personnes dont les communications privées ont été interceptées en vertu d'une autorisation ou dans des situations d'urgence sans mandat, lorsqu'il existe un risque imminent de préjudice.
[196] Article 788 de la loi sur l'administration de la justice : la notification doit être faite dès que possible si la police n'a pas, dans les 14 jours suivant l'expiration de la période pour laquelle l'interférence a été autorisée, donné suite à la notification. Les exceptions sont les cas où cela nuirait à l'enquête ou à l'enquête dans une autre affaire en cours concernant une infraction qui, selon la loi, peut constituer la base d'une ingérence dans le secret des communications, ou si la protection d'informations confidentielles sur les méthodes d'enquête de la police ou les circonstances s'opposent à la notification. Dans ces cas, le tribunal peut, à la demande de la police, décider que la notification sera omise ou reportée pendant une période déterminée, qui peut être prolongée par une décision ultérieure.
[197] Article 126 § 13 du code de procédure pénale.

Finlande[198], **Allemagne**[199], **Grèce**[200], **Italie**[201], **Corée**[202], **Kirghizstan**, **Liechtenstein**[203], **Lituanie**[204], **Luxembourg**[205], **République de Moldova**[206], **Pays-Bas**[207], **Macédoine du Nord**[208], **Saint-Marin**[209], **Serbie**[210], **République slovaque**[211], **Suisse**[212], **Ukraine**[213]. En l'absence d'exigences de notification, des plaintes pour des mesures ordonnées ou exécutées en violation de dispositions légales peuvent être déposées en **Autriche**[214], **Irlande**[215]. L'utilité de la notification en tant que recours dépend de la manière dont les exceptions sont interprétées dans la pratique (voir les paragraphes 120-122 ci-dessous).

67. Les pays suivants ont signalé l'existence d'un système de notification dans les cas de surveillance ciblée effectuée par les services de sécurité : **Belgique**[216], **Bosnie-Herzégovine**[217],

[198] L'article 60 de la loi sur les mesures coercitives prévoit la notification de l'utilisation de mesures coercitives secrètes.
[199] Article 101 du code de procédure pénale.
[200] En matière pénale, après l'expiration de la mesure et sur présentation d'une demande pertinente par la partie affectée, l'ADAE notifie à la partie affectée l'imposition de cette mesure dans un délai de soixante (60) jours, avec l'accord du procureur de la Cour suprême et à condition que l'objectif pour lequel la mesure a été ordonnée ne soit pas compromis (article 6 de la loi n° 5002/2022).
[201] Articles 268 et 269 du code de procédure pénale.
[202] Dans un délai de 30 jours à compter de la date de cessation des mesures.
[203] Article 104 § 2 du code de procédure pénale (StPO). L'art. 104 § 4 StPO prévoit en outre qu'un appel peut être interjeté auprès de la Cour supérieure dans les quatorze jours suivant la notification par le juge d'instruction. Cette décision peut faire l'objet d'une plainte individuelle auprès de la Cour constitutionnelle.
[204] Article 161 du code de procédure pénale.
[205] Article 88-4 § 6 du code de procédure pénale ; ils sont en outre informés qu'ils peuvent introduire un recours en annulation sur la base et dans les conditions de l'article 126.
[206] La notification peut être reportée jusqu'à la fin de l'enquête pénale. L'article 313 du code de procédure pénale prévoit un recours judiciaire contre les actions et actes illégaux du ministère public et des organes spéciaux d'enquête.
[207] Article 126b du code de procédure pénale. La notification doit avoir lieu dès que possible, mais n'a pas lieu lorsque cela est « raisonnablement impossible » ou lorsque les personnes sont automatiquement notifiées dans le cadre de procédures pénales en cours.
[208] Article 262 du code de procédure pénale.
[209] Loi n° 98 du 21 juillet 2009.
[210] Article 163 du code de procédure pénale
[211] Articles 114 et 115 du code de procédure pénale : les personnes concernées qui n'ont pas accès au dossier doivent être informées, dans un délai de trois ans à compter de la décision finale dans l'affaire pénale, qu'elles ont fait l'objet d'une surveillance et que les enregistrements ont été détruits. Elles doivent être informées de la possibilité de déposer auprès de la Cour suprême une requête en révision du mandat judiciaire autorisant la surveillance.
[212] Article 279 du code de procédure pénale : motif, type et durée de la surveillance au plus tard à la fin de la procédure préliminaire. Le tribunal des mesures obligatoires peut reporter la notification ou y renoncer si les résultats ne sont pas utilisés comme preuves dans la procédure judiciaire et si le report ou l'omission est nécessaire pour protéger des intérêts publics ou privés prépondérants.
[213] Article 253 du code pénal.
[214] Section 106 § 1 du code de procédure pénale.
[215] L'article 9 de la loi de 1993, l'article 11 de la loi de 2009 et l'article 10 de la loi de 2011 permettent à une personne de demander à un arbitre des plaintes d'examiner si une autorisation ministérielle d'interception a été accordée et, le cas échéant, si les exigences de la loi pertinente ont été respectées en ce qui concerne la demande. Le tiers statuant en référé peut examiner la légalité des mesures prises. Il est nommé par le Taoiseach pour un mandat de cinq ans. Jusqu'à présent, tous les titulaires de cette fonction ont été des juges en exercice de la Circuit Court. Le Referee a le pouvoir d'accéder à tous les documents officiels relatifs aux mesures prises. S'il conclut que la loi a été enfreinte, il doit en informer le demandeur par écrit et faire un rapport au Taoiseach. Il peut également annuler une autorisation ministérielle, ordonner à l'agence concernée de détruire les informations obtenues et recommander une indemnisation. Le système de recours se limite à vérifier si un mandat a été délivré correctement et ne prévoit pas de recours dans d'autres situations telles que la conservation ou la divulgation inappropriée de données par les services de télécommunications ou l'utilisation abusive de données par la Gardaí.
[216] Comme le prévoit l'article 2 § 3 de la L. R&S., les conditions sont les suivantes : un délai de plus de dix ans s'est écoulé depuis la fin de la méthode. Les conditions sont, *entre autres,* qu'une période de plus de dix ans se soit écoulée depuis la fin de la méthode, que la notification ne puisse pas porter atteinte à une enquête de renseignement et qu'elle ne puisse pas porter atteinte aux relations entre la Belgique et des institutions étrangères internationales ou supranationales.
[217] Article 77 de la loi sur l'Agence de renseignement et de sécurité, après la fin du contrôle, sauf si ces informations peuvent compromettre l'accomplissement des tâches de l'Agence ou l'achèvement de la procédure devant les autorités compétentes.

Danemark[218], **Estonie**[219], **Finlande**[220], **Allemagne**[221], **Corée**[222], **République de Moldova**[223], **Pays-Bas**[224], **Macédoine du Nord**[225], **Roumanie**[226], **Suisse**[227], **Ukraine**[228].

[218] Voir la note de bas de page 196 ci-dessus.
[219] Article 29 de la loi sur les autorités de sécurité : les exceptions sont les suivantes : 1) porter atteinte de manière significative aux droits et libertés d'une autre personne garantis par la loi ou mettre une autre personne en danger ; 2) mettre en danger la confidentialité des moyens, méthodes ou tactiques de l'autorité de sécurité ; 3) mettre en danger la source d'information ou une personne recrutée pour une coopération secrète ; 4) nuire à l'échange d'informations entre les autorités de sécurité ou à la coopération avec un État étranger ou une organisation internationale.
[220] Article 20 de la loi sur l'utilisation du renseignement sur le trafic des réseaux dans le renseignement civil et article 89 de la loi sur le renseignement militaire.
[221] Article 59 de la loi sur le service fédéral de renseignement et article 12 de la loi sur l'article 10.
[222] Voir note de bas de page 202 ci-dessus.
[223] Article 22 de la loi n° 59/2012, avec les exceptions suivantes : a) l'information constitue un risque accru pour la vie et la santé de la personne ; b) il est nécessaire d'effectuer une autre mesure d'enquête spéciale dans le même dossier spécial ; c) les résultats de la mesure d'enquête spéciale nécessitent des poursuites pénales. L'article 26 de la loi n° 59/2012 prévoit un mécanisme de recours.
[224] Article 59, paragraphe 1, de la loi sur les services de renseignement et de sécurité. En principe, les personnes concernées par l'application d'un pouvoir d'enquête doivent être informées cinq ans après la fin du pouvoir d'enquête. La notification n'est pas requise lorsque (a) les sources d'un service, y compris les services de renseignement et de sécurité d'autres pays, sont divulguées ; (b) les relations avec d'autres pays et avec des organisations internationales sont gravement compromises ; ou (c) une application spécifique d'une méthode (modus operandi) ou l'identité de la personne qui a aidé le service à appliquer la méthode est divulguée.
[225] L'article 51, paragraphe 6, de la loi sur la surveillance des communications impose au Conseil de contrôle civil d'informer rapidement le citoyen si un abus est détecté au cours de la surveillance. Si aucun abus n'est constaté, le citoyen est toujours informé, mais avec des détails limités afin de préserver la confidentialité.
[226] Article 21 § 2 de la loi n° 51/91 sur la sécurité nationale de la Roumanie. La notification est exclue si (a) elle pourrait conduire à compromettre l'exercice des fonctions officielles des organes de l'État chargés de la sécurité nationale en divulguant leurs sources, y compris celles des services de sécurité et de renseignement d'autres États ; b) elle pourrait affecter la défense de la sécurité nationale ; c) elle pourrait porter atteinte aux droits et libertés de tiers ; d) elle pourrait conduire à la divulgation des méthodes et moyens, y compris des techniques d'enquête spécifiques, utilisés dans l'affaire en question par les organes de l'État chargés de la sécurité nationale.
[227] Si la cible est située en Suisse, l'article 33 IntelSA prévoit que la personne surveillée doit être informée dans un délai d'un mois après la conclusion de l'opération. Les exceptions sont les suivantes : a. le report est nécessaire pour ne pas compromettre une recherche en cours ou une procédure judiciaire ; b. le report est nécessaire en raison d'un autre intérêt public prépondérant à la préservation de la sécurité intérieure ou extérieure, ou en raison des relations de la Suisse avec l'étranger ; c. l'information pourrait mettre en danger des tiers ; d. la personne concernée n'est pas atteignable. Si la personne visée se trouve à l'étranger, elle n'est pas informée de la mesure de renseignement.
[228] Article 25 de la loi ukrainienne « sur le renseignement », à condition que la fourniture de ces informations ne constitue pas une menace pour la sécurité nationale de l'Ukraine.

68. Au **Canada**, en **Grèce**[229], en **Irlande**[230], au **Kosovo**[231], au **Kirghizstan**, en **République slovaque**[232], aux **États-Unis**[233], si aucune obligation de notification n'existe dans le contexte des opérations de renseignement, des plaintes peuvent être déposées auprès des organes de contrôle/juridictions compétents.

G. Aperçu de la législation et de la pratique de certains États visant à prévenir l'utilisation abusive de logiciels espions

69. Il convient de noter que, dans certains États, des mesures législatives spécifiques ont été prises pour limiter le développement des logiciels espions ou pour réagir aux allégations d'utilisation abusive.

70. En **Autriche**, la Cour constitutionnelle a estimé le 11 décembre 2019[234] que la surveillance secrète de l'utilisation des systèmes informatiques constituait une ingérence grave dans le droit à la vie privée protégé par l'article 8 de la CEDH et n'était autorisée que dans des limites extrêmement étroites afin de protéger des intérêts juridiques tout aussi importants[235]. Il a donc déclaré inconstitutionnel l'article 135a du code de procédure pénale, adopté en 2018, qui autorise l'utilisation de logiciels espions pour lire des messages cryptés. L'article 135a, en liaison avec

[229] En avril 2024, le Conseil d'État grec a déclaré inconstitutionnel un amendement législatif de 2021 qui interdisait à l'ADAE d'informer les citoyens de la surveillance de l'État pour des raisons de « sécurité nationale ». Le Conseil d'État a estimé que l'interdiction générale d'informer les individus du fait qu'ils ont été soumis à une surveillance constituait une « restriction excessive » du droit à la vie privée et une menace pour l'État de droit. Grâce aux modifications législatives apportées en 2022, en vertu de l'article 4, paragraphe 3, de la loi n° 5002/2022, les personnes intéressées, si elles soupçonnent qu'elles ont été ciblées, doivent en faire la demande à l'ADAE, qui la soumet ensuite au PEJ. La loi prévoit toutefois que ces demandes ne sont recevables qu'après une période de trois ans à compter de la fin de la surveillance. Ni l'ADAE ni la PEJ ne peuvent en décider, mais un comité de trois membres, composé du procureur de la PEJ, du second procureur de haut rang chargé du dossier et du président de l'ADAE. Cette commission ne peut satisfaire à la demande que si elle estime que la divulgation ne compromet pas le champ d'application pour lequel la surveillance spécifique a été imposée. Plus important encore, si cette commission décide de notifier la personne intéressée, la loi prévoit qu'aucune autre information ne lui est communiquée, si ce n'est que ses communications ont bien été interceptées pendant la période divulguée. Néanmoins, toutes les informations concernant les raisons pour lesquelles la surveillance a été imposée ne sont pas divulguées.

[230] Voir note de bas de page 215 ci-dessus.

[231] L'article 39, paragraphe 2, de la loi sur l'Agence de renseignement du Kosovo dispose que les particuliers, les institutions et les tiers ont le droit de déposer une plainte contre l'Agence de renseignement du Kosovo auprès de l'institution du médiateur.

[232] Les personnes concernées peuvent également déposer une plainte constitutionnelle en vertu de l'article 127 de la Constitution. 127 de la Constitution. Le mécanisme de plainte constitutionnelle s'est récemment avéré essentiel pour combler une lacune de la PAIA, à savoir que les tribunaux régionaux exerçant un contrôle judiciaire en vertu de la PAIA n'ont pas le pouvoir d'ordonner spécifiquement la destruction d'enregistrements obtenus par le biais d'une surveillance illégale. Cette omission législative a été critiquée par la CourEDH dans son arrêt de 2021 dans l'affaire *Zoltán Varga c. Slovaquie*, nos 58361/12 et 2 autres, 20 juillet 2021. Dans le récent arrêt du 15 mai 2024 (III. ÚS 97/2012), la Cour constitutionnelle a spécifiquement ordonné - dans cette affaire - au Service d'information slovaque de détruire tous les enregistrements et autres documents encore existants obtenus par la surveillance illégale effectuée dans cette affaire et d'informer le plaignant de leur destruction.

[233] La FISA prévoit des recours individuels en cas d'actes illégaux commis par des fonctionnaires à l'encontre de personnes concernées. L'ECPA prévoit un recours en suppression en cas d'interception de communications électroniques et orales. Enfin, devant la Data Protection Review Court, les particuliers peuvent déposer des plaintes concernant des violations présumées de l'activité de surveillance du gouvernement américain lors de la collecte ou du traitement des données d'une personne.

[234] Cour constitutionnelle, Recueil des décisions 20356/2019 (11 décembre 2019).

[235] La Cour constitutionnelle a estimé que le « cheval de Troie fédéral » constituait une forme particulièrement intrusive de mesure de surveillance, notamment parce qu'une vue d'ensemble des données obtenues par la surveillance d'un système informatique permettait de tirer des conclusions, entre autres, sur les préférences personnelles et le mode de vie des utilisateurs individuels. En outre, elle a notamment (a) affectait un grand nombre de personnes ; (ii) il n'y avait aucune garantie que la mesure de surveillance ne serait mise en œuvre que si elle était utilisée pour poursuivre et résoudre des infractions suffisamment graves ; (iii) la mesure ne garantissait pas de manière adéquate la protection de la vie privée des personnes affectées par le cheval de Troie ; et (iv) il n'y avait aucune garantie qu'après l'approbation judiciaire *ex ante* de la mesure, le responsable de la protection juridique serait effectivement en mesure de contrôler de manière efficace et indépendante toute surveillance secrète en cours.

l'article 134 § 3a du code de procédure pénale, prévoyait (dans des cas précis et sous certaines conditions) l'autorisation de surveiller secrètement des messages cryptés en installant un logiciel espion - un « cheval de Troie fédéral » *(Bundestrojaner*) - sur un système informatique. Toutefois, ces dispositions ne sont finalement jamais entrées en vigueur car, le 11 décembre 2019, la Cour constitutionnelle autrichienne les a annulées.

71. Diverses formes d'évaluation de l'utilisation des logiciels espions, y compris par le biais de commissions d'enquête, ont eu lieu en **Belgique**[236], **Canada**[237], **Grèce**[238], **Italie**[239], **Pays-Bas**[240], **Pologne**[241], **Espagne**[242], **Suède**[243], **Suisse**[244], **États-Unis**[245].

---

[236] *Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel PEGASUS*, précitée.

[237] Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a préparé un rapport sur les outils d'investigation sur appareil utilisés par la Gendarmerie royale du Canada (GRC) et les questions connexes, citées ci-dessus. Le rapport examine les avantages et les risques liés à l'utilisation d'outils d'enquête sur les appareils et étudie les mesures législatives et non législatives qui pourraient être envisagées pour mieux réglementer ces types d'outils au Canada. Le rapport a constaté qu'il existe un vide législatif concernant l'utilisation des nouveaux outils d'investigation technologiques. Il conclut donc qu'un meilleur cadre législatif pour l'utilisation des outils d'investigation sur appareil par la GRC est nécessaire pour garantir l'utilisation appropriée de ces outils et la protection du droit à la vie privée des Canadiens.

[238] À la suite des incidents signalés en 2022 (voir le rapport de l'APCE, cité ci-dessus, exposé des motifs, §§ 31-35), une enquête parlementaire officielle a été menée pour examiner toute allégation d'utilisation de logiciels espions illégaux à des fins officielles. La commission a examiné comment les services de renseignement nationaux, dans le cadre de leur rôle, pouvaient mener des opérations de surveillance légalement autorisées, par des moyens proportionnés et conventionnels. Les conclusions de la commission ont été mises à la disposition de tous les membres du Parlement grec, sous le sceau de la confidentialité.

[239] *Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, précité, p. 41 et sf.

[240] En 2022, le Centre de recherche et de données du ministère néerlandais de la Justice et de la Sécurité a publié un rapport d'évaluation sur l'utilisation néerlandaise de logiciels espions par les autorités chargées de l'application de la loi. Il s'agit d'une étude empirique sur la mise en œuvre de ce pouvoir. L'étude a révélé qu'entre mars 2019 et mars 2021, le pouvoir a été émis dans 26 enquêtes criminelles. Il a été utilisé dans des enquêtes criminelles portant sur des formes plus graves de criminalité traditionnelle, telles que la (tentative de) meurtre, les affaires impliquant des stupéfiants, la falsification de documents, le blanchiment d'argent, les infractions sexuelles, les infractions de terrorisme et l'appartenance à une organisation criminelle. Le rapport précise que la police néerlandaise a utilisé un outil commercial dans la « grande majorité » des cas. Dans le contexte des services de renseignement et de sécurité, l'ensemble de la loi sur les services de renseignement et de sécurité a été évaluée en 2020, y compris l'utilisation de logiciels espions à l'article 45. Toutefois, l'accent n'a pas été mis sur la « surveillance ciblée », mais plutôt sur l'utilisation de logiciels espions dirigés vers des organisations et l'acquisition d'ensembles de données en vrac. Le nom du ou des outils commerciaux utilisés n'est pas public.

[241] En février 2024, une commission parlementaire spéciale a été créée pour enquêter sur l'utilisation de logiciels espions qui, selon le ministre polonais de la Justice, ont été utilisés sur près de 600 personnes entre 2017 et 2022. Le 10 septembre 2024, le Tribunal constitutionnel polonais a jugé que la commission était inconstitutionnelle dans le cadre de son activité.

[242] Suite aux révélations selon lesquelles 65 personnes ont été ciblées (dans ce qu'on appelle le « CatalanGate ») par des logiciels espions, (Rapport de l'APCE, précité, Exposé des motifs, §§ 36-42) une commission d'enquête spéciale a été créée : la Commission d'enquête parlementaire sur l'espionnage et l'intrusion dans la vie privée et l'intimité, par le biais des logiciels malveillants Pegasus et Candiru, de dirigeants politiques, d'activistes, d'avocats, de journalistes, d'institutions ainsi que de leurs familles et de leurs proches. *Comisión de Investigación sobre el espionaje e intromisión a la privacidad e intimidad, a través de los malware Pegasus y Candiru, a líderes políticos, activistas, abogados, periodistas, instituciones y sus familiares y allegados.* La commission est compétente pour a) examiner en détail l'implication des institutions de l'État dans les ingérences illégales présumées contre des dirigeants politiques, des institutions et d'autres personnes ; b) enquêter sur la responsabilité présumée et l'utilisation abusive d'organismes techniques dans tous les départements ministériels et le lien de ces organismes avec l'espionnage ; c) examiner en détail toutes les activités du ministère des affaires étrangères en relation avec les enquêtes menées de manière présumée illégale, sans être sub judice, des délégations de la Generalitat à l'étranger ; d) connaître les contrats, les coûts et les procédures de passation de marchés pour le développement et/ou l'achat présumé du logiciel Pegasus ou d'autres outils utilisés pour l'espionnage par des organismes officiels ; e) enquêter sur toutes les initiatives menées par les autorités de l'État afin de persécuter la dissidence politique ; f) proposer et soulever des mesures de réparation pour toutes les personnes touchées par des enquêtes illégales, ainsi que la responsabilité de l'utilisation abusive de l'appareil gouvernemental ; et g) proposer des mesures appropriées de contrôle, d'enquête et de prévention pour protéger la démocratie contre les abus de pouvoir de l'État et empêcher son utilisation contre les droits civils et politiques. Une deuxième commission, la commission d'enquête parlementaire « *sur la soi-disant* » *Opération Catalogne « et les actions du ministère de l'Intérieur pendant les gouvernements du Parti populaire en relation avec les irrégularités présumées liant de hauts fonctionnaires et des commandants de police à l'existence d'un complot d'autodéfense »* est compétente, entre autres, pour « connaître les contrats, les dépenses et les procédures de passation de marchés pour le développement et/ou l'achat présumé du logiciel appelé « Pegasus », ou d'autres outils prétendument utilisés pour l'espionnage par des organismes officiels ».

[243] L'autorisation initiale d'utiliser des logiciels espions a été précédée d'une commission d'enquête (comme c'est la norme pour toute nouvelle législation en Suède) - *Hemlig dataavläsning - ett viktigt verktyg i kampen mot allvarlig brottslighet*, SOU 2017:89. La loi introduite en 2020 devait s'appliquer pendant une période limitée (jusqu'en mars 2025). En 2023, le fonctionnement de la loi a été examiné par une autre commission d'enquête, *Hemlig*

72. Les **États-Unis** ont adopté des lois imposant des restrictions à Pegasus et aux catégories connexes de logiciels espions commerciaux. La loi publique 117-263 (50 USC §3232a) (2022)[246] impose aux agences de renseignement américaines de fournir des rapports annuels évaluant les menaces de contre-espionnage « et les autres risques pour la sécurité nationale » que les « logiciels espions commerciaux étrangers » font peser sur les Nations Unies. Elle autorise en outre le directeur du renseignement national à interdire aux agences de renseignement de « conclure un contrat ou un autre accord à quelque fin que ce soit avec une société qui a acquis, en tout ou en partie, un logiciel espion commercial étranger ». Public Law 117-81 (22 USC §2679e) (2021)[247] exige du secrétaire d'État qu'il dresse une liste des contractants qui ont « sciemment aidé ou facilité une cyberattaque ou mené une surveillance » contre les États-Unis ou contre : « *[d]es individus, y compris des militants, des journalistes, des hommes politiques de l'opposition ou d'autres individus, dans le but de supprimer la dissidence ou d'intimider les critiques, au nom d'un pays figurant dans les rapports annuels du département sur les pratiques en matière de droits humains, pour des actes systématiques de répression politique, notamment des arrestations ou détentions arbitraires, des actes de torture, des exécutions extrajudiciaires ou motivées par des considérations politiques, ou d'autres violations flagrantes des droits humains* ». Le décret 14093[248], promulgué en vertu de cette autorisation, interdit à toute agence ou service fédéral de faire un usage opérationnel d'un logiciel espion commercial lorsqu'ils déterminent*, entre autres,* « que le logiciel espion commercial présente des risques significatifs d'utilisation inappropriée par un gouvernement étranger ou une personne étrangère ». Le décret précise en outre les bases sur lesquelles une agence pourrait se fonder pour prendre une telle décision, y compris les utilisations en violation du droit international relatif aux droits humains.

73. Il est à noter que les gouvernements de l'Australie, de l'Autriche, du Canada, du Costa Rica, du Danemark, de l'Estonie, de la Finlande, de la France, de l'Allemagne, du Japon, de la Lituanie, des Pays-Bas, de la Nouvelle-Zélande, de la Norvège, de la Pologne, de la République d'Irlande, de la République de Corée, de la Suède, de la Suisse, du Royaume-Uni et des États-Unis ont approuvé une déclaration commune dans laquelle les signataires s'engagent à travailler collectivement pour lutter contre la prolifération et l'utilisation abusive des logiciels espions à usage commercial[249]. En particulier, les parties s'engagent à s'associer pour lutter contre l'utilisation abusive des logiciels espions et à : (i) s'efforcer d'établir des garde-fous et des procédures solides pour garantir que toute utilisation commerciale de logiciels espions est compatible avec le respect des droits humains universels, de l'État de droit, des droits civils et des libertés civiles ; (ii) empêcher l'exportation de logiciels, de technologies et d'équipements à

---

dataavläsning - utvärdering och permanent lagstiftning, SOU 2023:78. La conclusion générale de cette deuxième commission d'enquête était que la loi, même si elle n'avait été appliquée que peu de temps auparavant, avait été utilisée plus que prévu et qu'il s'agissait d'un outil d'enquête essentiel qu'il convenait de rendre permanent.

[244] La commission parlementaire compétente a demandé un rapport annuel de performance au SRC conformément à l'article 26 de la loi sur la sécurité intérieure et aux mesures contre les systèmes informatiques étrangers conformément à l'article 37 de la loi sur la sécurité intérieure depuis 2019. Dans son rapport, le SRC fournit une évaluation complète des avantages des mesures et aborde les aspects techniques et les questions de ressources. Les statistiques montrent que 9 opérations ont utilisé des logiciels informatiques spéciaux en 2023, contre 7 l'année précédente.

[245] Les États-Unis ont évalué les logiciels espions commerciaux et ont conclu, dans le décret du 27 mars 2023 (The White House, *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security*, 27 mars 2023), que « *[l]'exploitation croissante des données sensibles des Américains et l'utilisation inappropriée des technologies de surveillance, y compris les logiciels espions commerciaux, menacent le développement* » d'un « *écosystème* » technologique international [...]. En ce qui concerne les intérêts en matière de sécurité nationale et de politique étrangère, le décret note qu'il est utile de « *veiller à ce que la technologie soit développée, déployée et gérée conformément aux droits humains universels, à l'État de droit et aux autorisations, garanties et contrôles juridiques appropriés, de sorte qu'elle soutienne et ne porte pas atteinte à la démocratie, aux libertés civiles et à la sécurité publique* ».

[246] Disponible ici.

[247] Disponible ici.

[248] *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security*, cité ci-dessus.

[249] The White House, *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware*, 18 mars 2024. Liste des États telle que modifiée en dernier lieu le 22 septembre 2024.

des utilisateurs finaux susceptibles de les utiliser pour des cyberactivités malveillantes ; (iii) partager des informations sur la prolifération et l'utilisation abusive de logiciels espions commerciaux ; (iv) travailler en étroite collaboration avec les partenaires industriels et les groupes de la société civile afin d'éclairer leur approche, de contribuer à la sensibilisation et de fixer des normes appropriées, tout en continuant à soutenir l'innovation ; (v) engager d'autres gouvernements partenaires dans le monde à mieux aligner les politiques et les autorités de contrôle des exportations afin d'atténuer collectivement l'utilisation abusive des logiciels espions commerciaux et d'encourager la réforme de ce secteur.

V. Garanties minimales contre les abus de pouvoir

74. Comme indiqué ci-dessus, il est essentiel de veiller à ce que l'utilisation de logiciels espions ne confère pas aux États le pouvoir arbitraire et illégal de s'immiscer dans la vie privée des individus[250]. Les États sont liés par des obligations en vertu du droit international coutumier ainsi que par les obligations qu'ils ont contractées en adhérant aux traités internationaux relatifs aux droits humains, tels que la CEDH (et le PIDCP), qui visent à protéger les droits humains et à faire respecter l'État de droit. Pour que la surveillance au moyen de logiciels espions soit compatible avec l'article 8 de la CEDH et l'article 17 du Pacte international relatif aux droits civils et politiques, le cadre juridique qui l'autorise doit répondre à des exigences très strictes. S'appuyant sur la jurisprudence de la CourEDH en matière de surveillance ciblée, sur les rapports précédents de la Commission de Venise, sur d'autres normes européennes et internationales telles que la Convention 108+ ainsi que sur l'analyse comparative de la législation pertinente dans les États membres de la Commission de Venise, cette section donne un aperçu non exhaustif des grands principes qui devraient être respectés lors de l'utilisation de logiciels espions afin de se conformer à l'État de droit et aux normes en matière de droits humains.

A. Législation primaire accessible et prévisible

75. Étant donné que l'utilisation de logiciels espions constitue une ingérence dans le droit au respect de la vie privée, comme illustré ci-dessus, l'article 8, paragraphe 2, de la CEDH et l'article 17 du Pacte international relatif aux droits civils et politiques exigent qu'elle ne puisse être autorisée que si elle est réglementée de manière adéquate par la loi, c'est-à-dire qu'elle est « conforme à la loi ». Selon la CourEDH, cela « exige non seulement que la mesure contestée ait une certaine base en droit interne, mais renvoie également à la qualité de la loi en question, en exigeant qu'elle soit accessible à la personne concernée et prévisible quant à ses effets »[251].

76. La CourEDH a déclaré qu'en raison du risque d'abus inhérent à tout système de surveillance secrète, de telles mesures doivent être fondées sur une loi particulièrement précise, d'autant plus que la technologie disponible pour l'utilisation est de plus en plus sophistiquée[252]. Ainsi, l'utilisation d'un outil d'investigation particulier tel qu'un logiciel espion doit être réglementée par le droit *primaire*, c'est-à-dire par une loi[253]. Une telle exigence présente l'avantage de la légitimité démocratique, puisqu'elle permet à un législateur démocratiquement élu de déterminer les équilibres exacts qu'il convient d'établir entre des intérêts concurrents, et renforce la sécurité juridique[254]. La loi doit en outre répondre à des exigences de qualité : elle doit être accessible aux personnes concernées et prévisible quant à ses effets.

---

[250] Commission de Venise, CDL-AD(2016)007, précité, § 118.
[251] CourEDH, *Rotaru c. Roumanie* [GC], n° 28341/95, 4 mai 2000, § 52.
[252] CourEDH, *Uzun c. Allemagne*, no. 35623/05, 2 septembre 2010, § 61.
[253] *Voir, mutatis mutandis*, CourEDH, *Bykov c. Russie* [GC], no. 4378/02, 10 mars 2009, §76.
[254] En Suède, par exemple, il a été jugé nécessaire d'imposer une obligation légale de documenter toutes les décisions prises dans le cadre de mesures d'enquête secrètes. Il n'a pas été jugé suffisant que ces questions soient régies par des instructions internes du bureau du procureur ou de la police/de la police de sécurité. *Voir* prop. 2022/23:126, p. 181.

77. Compte tenu de ce qui précède, la qualité du droit national régissant l'utilisation des logiciels espions est une condition préalable essentielle pour réduire l'interférence des logiciels espions avec les droits à la vie privée et à la protection des données (et d'autres droits humains), ainsi que pour limiter le risque d'abus de pouvoir. Si les États décidaient d'utiliser une telle technique de surveillance, ils seraient tenus de veiller à ce que le cadre législatif soit conforme aux exigences de « qualité » du droit prévues notamment à l'article 8 de la CEDH.

1. Accessibilité de la législation

78. Dans les pays sur lesquels la Commission dispose d'informations, la loi régissant la surveillance ciblée est généralement une disposition du code de procédure pénale ou un acte législatif primaire spécifique consacré aux pouvoirs de surveillance/d'enquête[255]. Il s'agit d'actes officiellement publiés et accessibles au public.

2. Prévisibilité de la législation

79. Selon la CourEDH, une règle est « prévisible » si elle est formulée avec suffisamment de précision pour permettre à tout individu - le cas échéant avec des conseils appropriés - de régler sa conduite. Cette exigence de précision constitue une garantie essentielle contre l'arbitraire dans l'imposition de mesures restrictives, et cette protection est encore plus importante en ce qui concerne les mesures de surveillance secrète, en raison des risques accrus d'arbitraire dans de telles circonstances[256].

80. Toutefois, dans le contexte particulier de la surveillance, la prévisibilité ne signifie pas que les individus devraient être en mesure de prévoir quand les autorités sont susceptibles d'intercepter leurs communications afin qu'ils puissent adapter leur comportement en conséquence[257]. Dans le contexte de la surveillance visant à faire face aux menaces pour la sécurité nationale, l'imprécision du concept de sécurité nationale crée des problèmes particuliers, car une réglementation efficace exige un niveau élevé de précision, et une réglementation efficace est une condition préalable à un contrôle efficace.

81. La CourEDH a toutefois estimé que l'exigence de « prévisibilité » de la loi ne va pas jusqu'à obliger les États à adopter des dispositions légales énumérant en détail tous les comportements susceptibles d'entraîner la décision de soumettre un individu à une surveillance secrète pour des raisons de « sécurité nationale ». Par leur nature même, les menaces pour la sécurité nationale peuvent être de nature différente et peuvent être imprévues ou difficiles à définir à l'avance[258]. Dans le même temps, la CourEDH a également souligné que, dans les matières touchant aux droits fondamentaux, il serait contraire à l'État de droit, l'un des principes de base d'une société démocratique consacré par la Convention, qu'un pouvoir discrétionnaire accordé à l'exécutif dans le domaine de la sécurité nationale soit exprimé en termes de pouvoir illimité.[259] En outre, la CourEDH a estimé que les limites de la notion de sécurité nationale ne peuvent « être étendues au-delà de leur sens naturel ».[260] Par conséquent, la loi doit indiquer l'étendue du pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice avec suffisamment de clarté, eu égard au but légitime de la mesure en question, pour assurer à

[255] *Voir*, *entre autres*, l'Investigatory Powers Act 2016 au Royaume-Uni.
[256] CourEDH, *Malone c. Royaume-Uni*, n° 8691/79, 2 août 1984, § 68 : « *Puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la "loi" irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante - compte tenu du but légitime poursuivi - pour fournir à l'individu une protection adéquate contre l'arbitraire* » ; *voir aussi Segerstedt-Wiberg et autres c. Suède*, no 62332/00, 6 juin 2006, § 76.
[257] CourEDH, *Weber et Saravia c. Allemagne* (déc.), no. 54934/00, 29 juin 2006, § 93.
[258] CourEDH, *Kennedy c. Royaume-Uni*, précité, § 159.
[259] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 247.
[260] CourEDH, *C.G. et autres v. Bulgarie*, no. 1365/07, 24 avril 2008, § 43.

l'individu une protection adéquate contre les ingérences arbitraires[261]. La CourEDH a estimé que les États ne peuvent pas faire d'affirmations générales concernant la portée de la sécurité nationale qui rendraient impossible pour un requérant de contester efficacement l'allégation[262].

82. Comme nous l'avons vu plus haut, peu d'États réglementent spécifiquement les logiciels espions en tant qu'outils de surveillance ciblée, tandis que nombre d'entre eux les considèrent comme des « moyens techniques spéciaux » de surveillance sans prévoir de règles spécifiques. Si certains régimes juridiques nationaux sont assez détaillés et précis, d'autres ont tendance à s'appuyer sur des formulations relativement larges et ouvertes qui n'offrent pas nécessairement le degré de certitude et de précision requis. La Commission de Venise considère que, compte tenu du niveau d'intrusion particulièrement élevé des logiciels espions, et notamment du fait qu'ils peuvent impliquer une combinaison de différentes intrusions dans la vie privée, s'ils autorisent le déploiement de logiciels espions, les Etats devraient adopter une législation spécifique et adaptée avec un champ d'application *ratione personae*, *materiae* et *temporis* plus strict *par rapport à* d'autres mesures de surveillance ciblée. Cela devrait être une condition préalable à l'utilisation de logiciels espions par les États.

3. Nécessité d'établir une distinction entre les différents niveaux d'intrusion de la surveillance

83. Comme nous l'avons vu plus haut, toute une série de données à caractère personnel peuvent être mises à disposition par la surveillance au moyen de logiciels espions qui s'introduisent dans les appareils électroniques. La recherche comparative a montré que, dans les pays qui réglementent spécifiquement l'utilisation des logiciels espions, le type de données susceptibles d'être collectées diffère. Les données sur l'utilisation réelle des logiciels espions sont naturellement rares[263].

84. Une question particulière se pose dans les cas où la surveillance audio ou vidéo en direct d'un appareil est activée à distance. Au moins dans certains États, en dehors de la question spécifique des logiciels espions, l'interception en temps réel des communications (c'est-à-dire la surveillance audio d'une localité) est généralement perçue comme plus intrusive pour la vie privée que l'interception du contenu des télécommunications. L'activation d'un téléphone portable en tant que dispositif d'interception en temps réel est encore plus intrusive, puisqu'il suivra la cible où qu'elle aille et quoi qu'elle fasse. Dans ces États, il semble raisonnable que lorsque la législation prévoit des limites particulières à l'utilisation de l'interception des communications en temps réel par les services de police ou de sécurité, par exemple des seuils minimaux de gravité des infractions, des liens suffisamment étroits, sinon directs, avec une menace réelle et grave pour la sécurité nationale, ou des limites ou interdictions à l'utilisation de l'interception des communications en temps réel dans certains lieux (lieux de culte, médias, cabinets d'avocats, etc.), ces limites doivent également s'appliquer lorsque la police ou les services de sécurité demandent l'activation de la fonction de surveillance audio d'un téléphone ou d'un autre appareil. Lorsque les lois applicables prévoient que la surveillance audio/vidéo doit être limitée aux lieux où l'on peut supposer que le suspect séjourne, à définir dans le mandat d'autorisation, ces limites doivent également s'appliquer lorsqu'un logiciel espion est utilisé pour activer la surveillance audio[264].

85. Les logiciels espions peuvent présenter un défi particulier à cet égard car, pour des raisons techniques, il n'est pas toujours possible de limiter les informations ainsi recueillies. Etant donné

[261] CourEDH, *Liu c. Russie*, no. 42086/05, 6 décembre 2007, § 56, avec d'autres références.
[262] CourEDH, *Amie et autres c. Bulgarie*, no. 58149/09, 12 février 201, §§ 92 et 98.
[263] Voir par exemple la pratique suédoise, mentionnée dans la note de bas de page 74 ci-dessus, qui indique que l'utilisation de logiciels espions en Suède est presque exclusivement destinée à l'interception de télécommunications et à la collecte de données contenues dans l'appareil (c'est-à-dire pas pour la surveillance audio ou vidéo).
[264] *Voir, par exemple*, SOU 2023:78, cité ci-dessus, section 3.2.8, p. 73.

le caractère extraordinairement intrusif des logiciels espions par rapport à d'autres méthodes de surveillance, le filtrage des informations autorisées et non autorisées (ou pertinentes et non pertinentes) peut s'avérer techniquement difficile. La Commission de Venise recommande vivement aux Etats qui envisagent d'utiliser des logiciels espions de s'assurer qu'ils disposent, comme garantie obligatoire, d'équipes spécialisées, contrôlées et professionnelles capables de mettre en œuvre un filtrage efficace des informations, comme c'est le cas pour d'autres pratiques de collecte d'informations. Des exigences en matière de destruction devraient également être mises en place, soutenues par un contrôle externe solide, indépendant et doté de ressources suffisantes[265]. Ce contrôle externe doit être solide et fonctionnel, tant en théorie qu'en pratique.

86. S'agissant de la question de savoir s'il est justifié d'utiliser un logiciel espion pour activer la fonction de vidéosurveillance d'un appareil mobile, la Commission de Venise note que la vidéosurveillance en direct est sans doute l'une des fonctions les plus intrusives qu'un logiciel espion puisse activer. Compte tenu de son caractère intrusif, la législation devrait, si elle est autorisée, prévoir un cadre strict et clair pour son activation, notamment en imposant à l'organisme demandeur (et à l'organisme d'autorisation) l'obligation de spécifier le type d'informations recherchées, ainsi que les limites temporelles et géographiques de la surveillance. Les exigences en matière de destruction décrites ci-dessus doivent également s'appliquer.

87. La Commission de Venise estime que la législation nationale doit établir une distinction claire entre le type d'enquête dans le cadre de laquelle l'utilisation d'un logiciel espion peut être autorisée et les données personnelles de la cible ou d'autres personnes qui peuvent être recherchées. Cette distinction influe sur l'évaluation de la nécessité et de la proportionnalité des mesures prises. Cette évaluation doit notamment tenir compte de la durée des mesures et de l'intensité de leur intrusion dans la vie privée et/ou familiale d'une personne[266].

B. Portée *ratione personae* des mesures de surveillance ciblée

88. Une autre exigence standard découlant de la jurisprudence de la CourEDH est que la loi prévoie clairement que les mesures de surveillance ciblée soient principalement disponibles pour les seuls dispositifs de communication d'une personne qui est personnellement soupçonnée d'avoir commis une infraction grave ou de représenter une menace spécifique pour la sécurité nationale[267].

89. Selon la jurisprudence de la CourEDH, les mesures d'interception concernant une personne qui n'est pas soupçonnée d'une infraction ou qui constitue une menace pour la sécurité nationale

[265] Par exemple, l'approche suédoise consiste à établir deux ou plusieurs « couches » d'accès au matériel au sein de l'organisation chargée de l'enquête. Comme indiqué ci-dessus (paragraphe 14), l'utilisation de logiciels espions nécessite un groupe d'experts spécialisés. Ce groupe sera invariablement distinct du groupe chargé d'enquêter sur l'infraction spécifique ou la menace spécifique contre la sécurité nationale (agents des services de police ou de renseignement). Le groupe d'experts n'aura pas besoin de savoir (et ne saura généralement pas) quoi que ce soit sur l'enquête proprement dite. Le groupe d'experts rassemble le matériel, élimine tout ce qui n'est pas couvert par les paramètres de temps et de lieu définis dans l'autorisation, et détruit ce matériel excédentaire (voir plus loin les paragraphes 126-129). Un tel système à plusieurs niveaux peut réduire les risques de collecte d'un trop grand nombre d'informations. Toutefois, pour qu'il fonctionne, il faut évidemment que l'enquête porte sur un délit très spécifique ou une menace réelle et sérieuse pour la sécurité nationale et que l'autorisation fixe des limites temporelles et spatiales claires pour la surveillance. En outre, chaque accès au matériel recueilli doit faire l'objet d'un enregistrement infalsifiable. Ces journaux doivent à leur tour être supervisés par un ou plusieurs niveaux d'examen/contrôle interne*, voir* SOU 2023:78, cité ci-dessus, p. 190.

[266] Des exigences différentes doivent être établies en fonction du degré d'intrusion de la mesure recherchée, par exemple en fonction de la gravité de l'infraction. Comme on l'a vu plus haut (note de bas de page 71 et paragraphe 48), le code de procédure pénale néerlandais, tel que modifié en 2019, prévoit cinq types différents d'actes d'enquête qui peuvent être ordonnés à l'agent chargé de l'enquête en accédant à un appareil utilisé par un suspect - avec différents critères d'applicabilité *ratione materiae* ; en Suède (paragraphe 51 ci-dessus), la législation fait une différence entre la lecture de données impliquant et n'impliquant pas l'activation du microphone d'un appareil pour enregistrer le son - avec différentes catégories d'infractions qui justifient l'autorisation de la mesure.

[267] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 231.

peuvent, à titre exceptionnel, être justifiées au titre de l'article 8 de la Convention[268]. Toutefois, cela n'est possible que si certaines conditions strictes sont remplies, c'est-à-dire s'il existe des raisons particulièrement fortes de croire qu'une autre personne suspecte contactera l'appareil de l'autre personne, ou que des coordonnées matérielles sont susceptibles d'être trouvées sur l'appareil de cette autre personne[269]. La Commission de Venise considère que, si un Etat souhaite autoriser, à titre exceptionnel, la surveillance à de telles fins, cette possibilité devrait être associée à une autorisation préalable [judiciaire] et à un contrôle renforcé, par exemple une obligation spécifique de notification à l'organe de contrôle, combinée à une obligation procédurale pour l'organe de contrôle d'accorder une attention particulière à de tels cas[270]. En outre, le cercle des tiers susceptibles de faire l'objet de mesures d'interception devrait être précisé dans la décision en question, et l'autorité qui accorde l'autorisation devrait motiver suffisamment sa décision sur ce point[271].

90. D'autres limites peuvent consister à n'autoriser que l'examen de métadonnées historiques (stockées), et non de données ou de communications en temps réel, et à ne pas permettre l'activation de fonctions de surveillance audio ou vidéo[272].

91. Des problèmes particuliers se posent évidemment lorsqu'une organisation fait l'objet d'une enquête. Cela peut se produire tant pour la criminalité organisée que pour les menaces à la sécurité nationale. Dans la pratique, les organisations peuvent également être « fluides ». Une organisation « solide » est une organisation dont la structure et la composition du personnel sont plus ou moins fixes, tandis qu'une organisation « fluide » est plus informelle en termes de composition et de temps. La formulation des conditions d'utilisation des logiciels espions dans de telles circonstances doit faire l'objet d'une attention particulière, afin de ne pas compromettre les garanties offertes aux individus[273]. En raison de la nature plus floue de la sécurité nationale et des risques accrus d'abus qui en découlent, ces garanties sont particulièrement importantes dans ce cas.

92. Il convient de noter que certains pays interdisent la surveillance ciblée au moyen de logiciels espions sur les ordinateurs ou les téléphones d'un avocat, d'un journaliste ou d'un médecin[274]. Lorsque cela est exceptionnellement autorisé, la CourEDH et la Commission de Venise ont précédemment conclu que, si une surveillance était exercée à l'encontre de journalistes et d'avocats, des normes plus strictes devaient s'appliquer à ces opérations (seuils plus élevés avant d'approuver les opérations de surveillance, contrôle interne et externe plus exigeant, etc.)[275]

1. Utilisation de logiciels espions contre des journalistes et d'autres acteurs des médias

93. En ce qui concerne plus particulièrement le journalisme, il est bien établi que les outils de surveillance ne peuvent être appliqués que dans les circonstances les plus exceptionnelles. Les sources européennes et internationales ont largement reconnu que le rôle de chien de garde du

[268] CourEDH, *Greuter c. Pays-Bas* (déc.), no. 40045/98, 19 mars 2002.
[269] Il convient de souligner que ces résultats ont été obtenus dans le cadre d'une surveillance traditionnelle et non de mesures de surveillance intrusives, pour lesquelles un seuil plus élevé devrait sans doute être utilisé.
[270] Dans l'affaire *Haščák c. Slovaquie*, nos 58359/12, 27787/16 et 67667/16, 23 juin 2022, § 95, la CourEDH a estimé que la loi applicable n'offrait aucune protection aux personnes affectées de manière aléatoire par des mesures de surveillance secrète.
[271] CourEDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, précité, § 201.
[272] Voir, par exemple, la législation suédoise (paragraphe 51 ci-dessus) qui impose de telles limites à la section 5.
[273] *Voir par exemple* les recommandations formulées par le CTIVD néerlandais dans le rapport d'examen 53 sur l'utilisation du pouvoir d'enquête en matière de piratage par l'AIVD et le MIVD en 2015, 8 mars 2017, p. 17.
[274] Voir section IV.B ci-dessus.
[275] Commission de Venise, CDL-AD(2015)011, précité § 103 ; s'agissant des journalistes, *voir* CourEDH, *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, no. 39315/06, 22 novembre 2012 ; s'agissant des avocats, *voir* *Bersheda et Rybolovlev c. Monaco*, nos 36559/19 et 36570/19, 6 juin 2024, §§ 73-76. En ce qui concerne plus particulièrement les journalistes et les médias, voir également la législation européenne sur la liberté des médias, citée ci-dessus.

journalisme exige une prudence exceptionnelle lorsqu'il s'agit d'interférer avec ses fonctions. La CourEDH a noté que « *les autorités ne disposent que d'une marge d'appréciation limitée pour décider de l'existence d'un 'besoin social impérieux'* » afin de satisfaire à la nécessité d'une ingérence dans la vie privée et la liberté d'expression des journalistes[276]. La protection s'étend aux défenseurs de droits humain, aux organisations non gouvernementales qui recherchent et diffusent des informations dans l'intérêt du public[277] ainsi qu'aux universitaires, écrivains, blogueurs et autres personnes sur l'internet[278]. Les experts internationaux ont appelé à des « mesures globales » pour protéger les journalistes de la surveillance[279]. Le Conseil de l'Europe considère depuis longtemps que les ordres ou actions d'interception, la surveillance et les autres formes de recherche ou de saisie de données journalistiques « *ne devraient pas être appliquées si elles visent à contourner le droit des journalistes [...] de ne pas divulguer des informations identifiant leurs sources* »[280].

94. Ces principes ont un poids particulier dans le contexte des logiciels espions, d'autant plus que, comme l'a noté le Contrôleur européen de la protection des données, *« Pegasus ne devrait pas être assimilé aux outils d'interception « traditionnels » des forces de l'ordre »*[281]. Le Commissaire aux droits de l'homme du Conseil de l'Europe, évaluant l'extrême difficulté de limiter la portée des logiciels espions dans des cas particuliers, a noté que, même dans le contexte d'un cadre de garanties, « *il est virtuellement inimaginable que l'utilisation de Pegasus ou de logiciels espions équivalents puisse jamais être considérée comme conforme à la loi et aux garanties nécessaires telles qu'elles ont été définies par la Cour* »[282]. Le Haut Commissaire des Nations unies aux droits de l'homme a spécifiquement mis en garde contre les « effets paralysants » des logiciels espions sur le journalisme, qui pourraient entraîner une « érosion de la gouvernance démocratique »[283].

95. La législation européenne sur la liberté des médias de l'Union européenne, qui est entré en vigueur en 2024 et s'appliquera à partir d'août 2025, a cherché à résoudre ce problème. L'article 4 § 3 (c) de l'Acte prévoit, en règle générale, que les logiciels espions ne peuvent être déployés contre les fournisseurs de services de médias ou d'autres personnes, ce qui pourrait entraîner la divulgation de sources et de communications. Il ne prévoit de dérogation à cette protection standard que dans les cas suivants (i) les autorités démontrent l'existence d'une raison impérieuse d'intérêt public ; (ii) il existe une autorisation ex ante d'une autorité judiciaire ou d'une autorité décisionnelle indépendante et impartiale ou, dans des cas exceptionnels et urgents, une autorisation ultérieure d'une telle autorité ; (iii) l'enquête concerne des infractions particulièrement graves et implique une personne visée ;[284] (iv) aucune autre mesure moins restrictive ne serait adéquate et suffisante pour obtenir les informations recherchées.

---

[276] CourEDH, *Stoll c. Suisse* [GC], n° 69698/01, 10 décembre 2007, § 105.
[277] CourEDH, *Animal Defenders International c. Royaume-Uni*, no. 48876/08, 22 avril 2013, §103.
[278] CourEDH, *Magyar Helsinki Bizottság c. Hongrie*, n° 18030/11, 8 novembre 2016, § 168.
[279] *Voir par exemple la* Déclaration conjointe sur la liberté des médias et la démocratie, le Rapporteur Spécial des Nations Unies (ONU) sur la promotion et la protection du droit à la liberté d'opinion et d'expression, le représentant de l'Organisation pour la sécurité et la coopération en Europe (OSCE) sur la liberté des médias, le rapporteur spécial de l'Organisation des États américains (OEA) sur la liberté d'expression et le rapporteur spécial de la Commission africaine des droits de l'homme et des peuples (CADHP) sur la liberté d'expression et l'accès à l'information en Afrique, 2 mai 2023.
[280] Conseil de l'Europe, *Recommandation n° R (2000) 7 du Comité des Ministres aux Etats membres sur le droit des journalistes de ne pas révéler leurs sources d'information*, Annexe : Principe 6, 8 mars 2000.
[281] Contrôleur européen de la protection des données, *Remarques préliminaires sur les logiciels espions modernes*, 15 février 2022.
[282] *Des logiciels espions très intrusifs menacent l'essence même des droits humains*, cités plus haut.
[283] *Le droit à la vie privée à l'ère du numérique*, précité.
[284] L'article 4, paragraphe 3, point c), de la législation désigne ces personnes comme « *les fournisseurs de services de médias, leur équipe rédactionnelle ou toute personne qui, en raison de ses relations régulières ou professionnelles avec un fournisseur de services de médias ou son équipe rédactionnelle, pourrait disposer d'informations se rapportant à des sources journalistiques ou des communications confidentielles ou permettant de les identifier* ».

96. Les pouvoirs très intrusifs offerts par les logiciels espions menacent le travail des journalistes et la volonté des sources de leur parler. Le scandale Pegasus a montré que les journalistes étaient apparemment ciblés simplement parce qu'ils sont journalistes, ce qui est inacceptable dans une société démocratique. La Commission de Venise considère que la législation devrait définir de manière étroite les cibles possibles des mesures de surveillance et prévoir que certaines catégories de personnes dont les interactions peuvent être protégées par le secret professionnel, ainsi que les journalistes, sont en principe exclues, avec certaines exceptions limitées. Lorsqu'il est allégué, sur la base de motifs justifiés, que ces personnes commettent une infraction spécifique, définie et grave et qu'elles représentent une menace spécifique définie pour la sécurité nationale, et qu'une enquête judiciaire est donc nécessaire, la Commission de Venise considère, conformément à la jurisprudence de la Cour européenne des droits de l'homme, que des normes fortement renforcées doivent s'appliquer, y compris des seuils plus élevés avant l'approbation des opérations de surveillance et un contrôle interne et externe plus exigeant (voir le paragraphe 92 ci-dessus).

C. Champ d'application *ratione materiae* des mesures de surveillance ciblée

97. Il est également important que la législation définisse clairement la nature des infractions pouvant donner lieu à une ordonnance d'interception. Comme indiqué précédemment, les conditions de clarté et de prévisibilité de la loi n'exigent pas des États qu'ils définissent de manière exhaustive les infractions spécifiques pouvant donner lieu à une interception. Toutefois, il convient de fournir suffisamment de détails sur la nature des infractions en question[285]. Si les États ont en principe le pouvoir souverain de déterminer ce qui constitue ou non une infraction grave en droit national, la CourEDH a clairement indiqué qu'il s'agit d'un sous-ensemble plus restreint de l'ensemble des infractions : un État n'est pas libre d'élargir cette catégorie de manière à ce qu'elle couvre en pratique la majorité de toutes les infractions[286]. Cela vaut *a fortiori* pour les mesures de surveillance intrusives[287].

98. En ce qui concerne les menaces pour la sécurité nationale, comme illustré ci-dessus, l'exigence de « prévisibilité » de la loi ne va pas jusqu'à obliger les États à adopter des dispositions légales énumérant en détail tous les comportements susceptibles d'entraîner une décision de soumettre un individu à une surveillance secrète pour des raisons de « sécurité nationale ». Toutefois, la portée de tout pouvoir discrétionnaire conféré aux autorités compétentes doit être strictement définie, notamment en ce qui concerne la portée matérielle et personnelle de l'autorisation préalable [judiciaire] (voir les conclusions de la CourEDH au paragraphe 81 ci-dessus). En outre, comme déjà mentionné, un contrôle efficace devient encore plus important. La CJUE a élaboré des normes spécifiques en matière de sécurité nationale, estimant notamment que les États membres, lorsqu'ils prennent des mesures pour sauvegarder la sécurité nationale, doivent être en mesure de démontrer qu'il existe des motifs suffisamment solides de croire qu'ils sont confrontés à une menace grave pour la sécurité nationale, dont il est établi qu'elle est réelle et actuelle ou prévisible[288] ; ils doivent prouver qu'il est nécessaire de recourir à une dérogation au droit de l'UE pour sauvegarder la sécurité nationale[289] et que la

[285] CourEDH, *Kennedy c. Royaume-Uni*, précité, § 159.
[286] CourEDH, *Iordachi et autres c. Moldova*, n° 25198/02, 10 février 2009, § 44.
[287] À titre d'exemple, la législation européenne sur la liberté des médias prévoit que les logiciels de surveillance intrusifs ne doivent être déployés sur les professionnels des médias que s'ils interviennent dans le cadre d'enquêtes sur des infractions énumérées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil, punies dans l'État membre concerné d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans, ou dans le cadre d'enquêtes sur d'autres infractions graves punies dans l'État membre concerné d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins cinq ans, telles que déterminées par le droit national de cet État membre, et à condition qu'aucune autre mesure moins restrictive ne soit adéquate et suffisante pour obtenir les informations recherchées.
[288] CJUE, *La Quadrature du Net*, précité, § 137.
[289] Voir, *mutatis mutandis*, CJUE, *Commission européenne c. République de Pologne e.a.*, affaires jointes C-715/17, C-718/17 et C-719/17, §§152 et 159.

nécessité de protéger la sécurité nationale n'aurait pas pu être satisfaite en appliquant les dispositions pertinentes du droit de l'UE.[290]

D. Limites temporelles des mesures de surveillance ciblée

99. La question de la durée totale des mesures de surveillance ciblée peut être laissée à l'appréciation des autorités chargées d'émettre et de renouveler les mandats d'interception, à condition qu'il existe des garanties adéquates, telles qu'une indication claire en droit interne de la période après laquelle un mandat d'interception expirera, des conditions dans lesquelles un mandat peut être renouvelé et des circonstances dans lesquelles il doit être révoqué[291]. La CourEDH a critiqué la législation nationale qui ne prévoyait pas de limite claire dans le temps pour l'autorisation d'une mesure de surveillance ciblée[292]. La CJUE a estimé que lorsqu'un État membre adopte une mesure législative prévoyant la collecte en temps réel de données relatives au trafic et de données de localisation ciblées sur un individu, celle-ci doit être limitée dans le temps, à ce qui est « strictement nécessaire ».[293] La Commission de Venise considère que plus une ingérence dans la vie privée se prolonge, plus ses effets sur les droits de l'homme et les libertés sont importants, ce qui nécessite une justification plus solide. Les longues périodes seront plus difficiles à justifier en vertu des principes de nécessité et de proportionnalité.

100. Outre la question de la durée, la Commission de Venise considère qu'il est également nécessaire dans ce contexte de tenir compte du degré d'intrusion dans la vie privée d'une mesure de surveillance. Plus une mesure est intrusive, plus les périodes d'autorisation devraient être courtes. Dans tous les cas où une longue période de surveillance est autorisée, ou lorsqu'une courte période doit être renouvelée (fréquemment et à plusieurs reprises), il est particulièrement important d'imposer à l'organe d'enquête l'obligation d'informer immédiatement la juridiction ou l'organe d'autorisation et/ou l'organe de contrôle si les conditions changent au cours de l'enquête. Il est en effet possible qu'une enquête lancée de bonne foi sur un délit grave pour lequel la surveillance intrusive est autorisée se transforme, avec le temps, en une enquête sur un délit moins grave pour lequel la surveillance intrusive n'est pas autorisée - dans ce cas, la forme de surveillance la plus intrusive devrait être immédiatement interrompue.

101. Les délais peuvent également s'appliquer dans un autre sens, à savoir les clauses de caducité, qui précisent que la législation relative à la surveillance expirera après un certain nombre d'années (voir par exemple la note de bas de page 243 ci-dessus). Cette disposition peut être combinée avec l'obligation de mener une enquête officielle sur la manière dont la législation a été utilisée et de rendre cette enquête publique (du moins dans la mesure du possible). Il s'agit là d'une bonne pratique qui, espérons-le, servira à rassurer le public sur le fait que les pouvoirs ne sont pas utilisés de manière abusive.

E. Test de la moindre intrusion possible

102. En ce qui concerne les conditions qui doivent être inscrites dans la loi, une exigence standard pour toutes les méthodes d'enquête spéciales est d'imposer un test de « moyens les moins intrusifs » - il s'agit d'un corollaire naturel du principe de proportionnalité. La CourEDH l'a précisé dans le cadre de l'interception de masse[294], mais cela s'applique *mutatis mutandis* aux mesures de surveillance ciblée. L'organe requérant doit ainsi démontrer à l'organe d'autorisation que les informations recherchées dans le cadre de l'enquête ne peuvent être obtenues par des moyens moins intrusifs. Ce faisant, il convient d'évaluer les éventuels effets positifs d'un

[290] Voir, *mutatis mutandis*, CJUE, *Commission européenne c. République d'Autriche (« Imprimerie d'État »)*, affaire C-187/16, §§ 78-80.
[291] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 250.
[292] CourEDH, *Iordachi et autres c. Moldova*, précité, § 45.
[293] CJUE, *La Quadrature du Net*, précité, § 189.
[294] CourEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], précité, § 448.

traitement de données particulier et spécifique, de préférence par le biais d'un ensemble de sources de preuves indépendantes et de pratiques comparatives.

103. La procédure d'autorisation et le contrôle doivent être rigoureux, afin d'éviter que ces exigences ne deviennent de simples formalités plutôt que des exigences juridiques substantielles devant être clairement satisfaites. Il ne s'agit pas simplement d'une question de sécurité juridique. Étant donné que l'utilisation de logiciels espions tend encore à être un processus très gourmand en ressources, les services de police ou de sécurité chargés de l'enquête devraient également avoir tout intérêt à gérer efficacement leurs ressources[295].

F. Autorisation et contrôle des mesures de surveillance ciblée par un organe judiciaire ou un autre organe indépendant

104. Selon la jurisprudence de la CourEDH, le contrôle et la supervision des mesures de surveillance secrète peuvent intervenir à trois stades : lorsque la surveillance est ordonnée pour la première fois, pendant qu'elle est mise en œuvre ou après sa cessation. En ce qui concerne les deux premières étapes, la nature et la logique mêmes de la surveillance secrète imposent que non seulement la surveillance elle-même, mais aussi le contrôle qui l'accompagne, soient effectués à l'insu de l'individu. Par conséquent, étant donné que les individus seront nécessairement empêchés d'exercer un recours effectif de leur propre chef ou de participer directement à toute procédure de réexamen, il est essentiel que les procédures mises en place fournissent elles-mêmes des garanties adéquates pour la sauvegarde de leurs droits. Dans un domaine où l'abus de pouvoir est potentiellement si facile et peut avoir des conséquences si néfastes pour l'ensemble d'une société démocratique, la Cour a jugé qu'il est en principe souhaitable de confier le contrôle de surveillance à un juge, le contrôle juridictionnel offrant les meilleures garanties d'indépendance, d'impartialité et de régularité de la procédure[296].

105. Une procédure d'autorisation purement politique, c'est-à-dire dans laquelle la police ou une agence de sécurité demande l'autorisation au ministre responsable, n'est pas acceptable au regard de la CEDH ([297]) et du Pacte international relatif aux droits civils et politiques. Il est toutefois possible de combiner les deux procédures, l'autorisation étant demandée à un ministre du gouvernement (qui se concentrerait vraisemblablement sur la question de l'aptitude) tandis que la question de la légalité est déterminée par le tribunal. Comme la CourEDH l'a jugé à plusieurs reprises, à commencer par l'affaire *Klass*, l'autorisation judiciaire est préférable, car elle offre les meilleures garanties d'indépendance, d'impartialité et de régularité de la procédure[298]. Toutefois, dans certains domaines, il peut y avoir des raisons de remplacer un tribunal par un organe d'autorisation expert, à condition que cet organe satisfasse à des normes élevées d'indépendance. La Commission de Venise considère, conformément à la pratique de la CourEDH, que l'existence d'un organe d'autorisation expert peut être plus justifiée en ce qui concerne la surveillance de masse,[299] mais que l'autorisation judiciaire doit être préférée pour la surveillance ciblée. Cela n'exclut pas un certain degré de spécialisation du ou des tribunaux qui peuvent autoriser l'utilisation de logiciels espions (voir le paragraphe 111 ci-dessous).

---

[295] *Outils d'enquête sur les appareils utilisés par la Gendarmerie royale du Canada (GRC) et questions connexes*, précité, p. 21

[296] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 233.

[297] CourEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], précité, § 351. Voir également un jugement récemment publié (en maltais uniquement) du premier tribunal de la Cour civile de Malte (agissant en tant que Cour constitutionnelle) qui a estimé que le droit à un procès équitable d'un requérant dont le téléphone avait été mis sur écoute avait été violé car les écoutes avaient été effectuées en vertu d'un mandat délivré par l'exécutif plutôt que par une autorité judiciaire.

[298] Voir CourEDH, *Klass et autres c. Allemagne, no. 5029/71, 6 septembre 1978, §§ 55-56,* et *Roman Zakharov c. Russie* [GC], précité, § 233.

[299] Voir Commission de Venise, CDL-AD(2015)010, précité, §§ 210, 250; CDL-AD(2015)011, précité, §§ 24, 115-122 ; voir aussi CourEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], précité, § 351, citant l'arrêt de chambre *Big Brother Watch et autres c. Royaume-Uni*, nos 58170/13 62322/14 24960/15, 13 septembre 2018, §§ 318-320.

106. Dans le contexte de la surveillance secrète, la CourEDH a estimé que, dans des cas d'urgence exceptionnels, la mesure de surveillance ciblée pouvait être mise en œuvre sans autorisation préalable, à condition que le tribunal ou l'organe indépendant compétent l'autorise dans un bref délai[300]. Récemment, la CourEDH a estimé qu'un délai de cinq jours pour qu'une juridiction accorde ou rejette *a posteriori* la demande de mesure de surveillance ciblée n'offrait pas de garanties suffisantes, car l'application de la procédure d'autorisation d'urgence n'était justifiée que par le risque de perte des preuves, et non par la gravité ou la nature de l'infraction. La Cour a estimé que, compte tenu des dangers que le recours à une telle procédure d'urgence non judiciaire comporte pour la sphère privée de l'individu soumis à une surveillance secrète, la législation applicable devrait contenir des garanties suffisantes pour assurer que son utilisation est parcimonieuse et limitée à des cas dûment justifiés, y compris des garanties contre l'utilisation répétée de la mesure en question[301].

1. Critères d'évaluation par la juridiction habilitée/l'organisme indépendant

107. La CourEDH a souligné que le tribunal ou l'organe indépendant qui autorise la mesure doit être en mesure d'en évaluer le caractère raisonnable dans le cas d'espèce et elle a constaté des violations de la CEDH dans des cas où rien n'indiquait que les juges qui avaient délivré les mandats avaient exercé une fonction de contrôle[302].

108. À cet égard, la CourEDH examine également le champ d'application du contrôle (si le juge applique un test de « nécessité » ou de « proportionnalité ») et le contenu de l'autorisation d'interception. Il est courant d'exiger de l'organisme d'enquête qu'il fournisse au tribunal ou à l'organe d'autorisation indépendant la base de l'autorisation, généralement exprimée par des indications « concrètes » ou « factuelles » (d'un certain niveau) d'une infraction pénale en cours ou imminente, ou d'une menace pour la sécurité nationale, ainsi que par une sorte de seuil de preuve.

109. La surveillance ciblée est parfois autorisée non seulement pour enquêter sur des infractions ou des menaces passées ou présentes (en cours) pour la sécurité nationale, mais aussi sur des infractions ou des menaces potentielles et futures pour la sécurité nationale. La Commission de Venise estime qu'en général, la législation devrait prévoir des normes matérielles et des seuils de preuve plus élevés lorsqu'il s'agit d'autoriser l'utilisation de logiciels espions pour enquêter sur des infractions ou des menaces imminentes/futures (par exemple, en ce qui concerne les indices concrets). Une autorisation judiciaire ou indépendante qui n'examine pas ces questions cruciales ne constitue pas une véritable garantie. Toutes ces exigences de fournir des indications concrètes/factuelles et de satisfaire à des seuils de preuve donnés doivent être accompagnées de l'obligation pour l'autorité requérante de documenter ces éléments dans la demande. Cela est nécessaire, d'une part, parce que les conditions pourraient bien changer au cours de l'enquête et, d'autre part, parce que cela sera nécessaire pour le contrôle de suivi qui doit avoir lieu.

110. Enfin, l'autorité requérante doit examiner en permanence la persistance des motifs de la surveillance et informer l'organe d'autorisation en cas de modification des motifs justifiant l'application de la mesure. Si ces raisons n'existent plus, la surveillance doit cesser immédiatement[303].

2. Spécialisation des organes judiciaires et autres organes indépendants

111. Certains États ont prévu un certain degré de spécialisation, par exemple en ce qui concerne les procureurs et/ou les tribunaux, ou, comme indiqué ci-dessus, en créant des organismes

[300] CourEDH, *Ekimdzhiev et autres c. Bulgarie*, n° 70078/12, 11 janvier 2022, §323.
[301] CourEDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, précité, § 208.
[302] CourEDH, *Ekimdzhiev et autres c. Bulgarie*, précité, §§307-322 ; *Haščák c. Slovaquie*, précité ; *Zoltán Varga c. Slovaquie*, précité.
[303] *Voir par* exemple, en République slovaque, les articles 4 § 6 et 6 § 1 de la PAIA.

d'autorisation indépendants spécialisés dans la surveillance ciblée. Différents niveaux d'autorisation peuvent également être prévus en fonction des différents types d'enquête/de données recherchées ou de la manière dont la surveillance est effectuée, physiquement ou à distance[304]. Comme nous l'avons déjà indiqué (note de bas de page 265 ci-dessus), des unités spécialisées existent également au sein de certains services répressifs. Ces unités fournissent le soutien technique nécessaire au déploiement de logiciels de surveillance intrusive, mais aident également les unités opérationnelles à satisfaire aux exigences légales requises pour l'utilisation de ces logiciels. La concentration des compétences auprès d'un organe spécialisé particulier au sein des services répressifs ou des services de sécurité et de renseignement peut présenter des avantages en termes d'efficacité et de contrôle. En outre, comme nous l'avons également noté, cela peut contribuer à préserver la confidentialité dans le traitement des informations obtenues vis-à-vis d'autres parties de l'organisation chargée de l'enquête). En tout état de cause, des règles doivent exister et être strictement respectées pour limiter les informations qui peuvent être stockées, analysées et communiquées à d'autres services de l'organisme d'enquête ou à l'extérieur de celui-ci[305].

112. Comme la Commission de Venise l'a noté précédemment, un certain degré de spécialisation peut présenter des avantages dans la mesure où, grâce à une répétition fréquente, les personnes impliquées dans le processus d'autorisation deviennent plus expertes en la matière. Ainsi, un organisme plus expert pourrait être plus enclin à fixer des conditions plus nombreuses et plus efficaces pour les autorisations qu'il délivre. Dans le même temps, il est important d'éviter le « durcissement des affaires » (une tendance des juges spécialisés à s'identifier aux responsables de la sécurité) et de maintenir la confiance du public dans l'intégrité du système d'autorisation[306].

3. Défenseurs de la vie privée et de la sécurité

113. La Commission de Venise a précédemment constaté que le fait que l'autorisation des mesures de surveillance soit effectuée à l'insu de l'individu peut, dans une certaine mesure, être compensé par la présence, dans la procédure d'autorisation, de défenseurs de la vie privée, c'est-à-dire de professionnels du droit qui représentent les intérêts des personnes et des organisations ciblées dans la procédure d'autorisation[307]. La question de savoir si ces avocats peuvent constituer une véritable garantie dans la procédure dépend d'un certain nombre de facteurs. Le procureur (ou l'organe requérant) sera généralement en possession de beaucoup plus d'éléments de preuve. Un avocat soumis à un contrôle de sécurité n'agit pas directement pour le suspect et ne peut évidemment pas le consulter. Il se peut que l'avocat ne dispose que de très peu de temps pour se familiariser avec le dossier et qu'il soit donc désavantagé sur le plan de la procédure par rapport au procureur. En Suède, une commission d'enquête a constaté que l'obligation d'impliquer un avocat ayant fait l'objet d'une enquête de sécurité n'aboutissait que rarement, voire jamais, à un refus d'autorisation[308]. D'un autre côté, le mécanisme peut encore avoir une certaine valeur dans la mesure où il peut conduire à l'imposition de conditions visant à minimiser l'intrusion dans la vie privée, pour la cible ou d'autres personnes affectées par la

[304] Aux Pays-Bas, le Conseil des procureurs généraux (la direction nationale du ministère public) autorise l'utilisation de logiciels espions dans le cadre d'enquêtes criminelles. En Suisse, pour les mesures de renseignement effectuées sur le territoire de la Fédération, la mesure de renseignement doit être autorisée par le président d'une section spéciale du Tribunal administratif fédéral. En outre, la mesure doit être approuvée par le ministre de la défense après consultation du ministre des affaires étrangères et du ministre de la justice ; le Conseil fédéral (le gouvernement suisse) peut être saisi des cas d'une importance particulière. En Espagne, un magistrat de la Cour suprême (de la chambre administrative ou pénale) et un substitut sont désignés pour autoriser les interceptions de communications par les services de renseignement. En Suède, l'article 14 de la loi (2020:62) sur la lecture des données secrètes prévoit que dans des cas spécifiques liés à des personnes soupçonnées de terrorisme étranger, un tribunal spécialisé (le tribunal de district de Stockholm) est compétent.
[305] CourEDH, *Centrum för Rättvisa c. Suède* [GC], précité, § 276.
[306] Commission de Venise, CDL-AD(2015)010, précité, §§ 221-223.
[307] Commission de Venise, CDL-AD(2015)011, précité, § 100 ; CDL-AD(2016)012, précité, § 97.
[308] Voir l'enquête officielle suédoise sur la surveillance secrète, SOU 2012:44.

surveillance. En outre, il peut formaliser le processus d'obtention de l'autorisation, en précisant que c'est à l'organisme demandeur qu'il incombe de démontrer la nécessité du recours à la surveillance et que toutes les conditions de la surveillance sont remplies.

G. Systèmes nationaux de contrôle

114. Le contrôle est essentiel pour contribuer à garantir que les logiciels espions - qui entraînent des interférences aussi importantes avec les droits à la vie privée et à la protection des données - sont utilisés conformément à la loi. Le contrôle est également nécessaire pour se prémunir contre les abus des services de police et de renseignement et pour garantir que ces services remplissent leur mandat et utilisent leurs pouvoirs et leurs ressources de manière appropriée et efficace.

115. La Commission de Venise a souligné, dans le contexte du contrôle des agences de sécurité, que la principale garantie contre les abus de pouvoir est le contrôle interne effectué par les services de sécurité eux-mêmes, afin de s'assurer que le personnel travaillant dans les agences est attaché aux valeurs démocratiques de l'État et au respect des droits humains[309]. Une remarque similaire peut être faite en ce qui concerne l'application de la loi.

116. Néanmoins, un contrôle externe est également nécessaire pour rassurer le parlement et le public sur le fait que les procédures de contrôle interne sont suivies correctement[310]. Bien qu'il soit en principe souhaitable de confier le contrôle d'autorisation à un tribunal, un contrôle *post hoc* par des organes non judiciaires peut être considéré comme compatible avec la CEDH, à condition que l'organe de contrôle soit indépendant des autorités chargées de la surveillance et qu'il soit investi de pouvoirs et de compétences suffisants pour exercer un contrôle effectif et continu[311], et pour assurer une protection efficace contre les abus, y compris des pouvoirs d'enquête et de réparation. Les mandats des organes de surveillance se complètent, de sorte que, dans l'ensemble, ils assurent un contrôle continu et des garanties appropriées. Cette complémentarité peut être obtenue par une coopération informelle entre les organes de contrôle ou par des moyens statutaires[312]. Dans le cadre de l'« interception de masse », la CourEDH a souligné la nécessité de garanties « de bout en bout », couvrant l'ensemble du processus de surveillance, y compris la question du transfert d'informations/de matériel à d'autres organisations que celle qui effectue l'enquête, dans son propre État et dans d'autres États[313].

117. Il existe une différence entre le contrôle de la sécurité/du renseignement et le contrôle de la police/de l'application de la loi. Les opérations de surveillance des forces de l'ordre tendent à déboucher sur des poursuites judiciaires et il existe donc, en fin de compte, une possibilité de contrôle judiciaire *post hoc.* Ce n'est généralement pas le cas pour les activités de sécurité et de renseignement, d'où la nécessité de mettre en place des organes de contrôle et de surveillance spécialisés. Comme nous l'avons vu plus haut, l'existence de commissions parlementaires de contrôle est une caractéristique commune du système de contrôle de la sécurité/du renseignement dans les États membres[314]. Les parlements jouissent d'une légitimité démocratique et peuvent demander des comptes à l'exécutif sur la manière dont il dirige et supervise les activités des services de sécurité[315]. Cela dit, la Commission de Venise a déjà mis en garde contre les lacunes d'un contrôle purement parlementaire[316]. Les organes d'experts, qui assurent le contrôle des activités des services de renseignement dans un certain nombre d'Etats,

[309] Commission de Venise, CDL-AD(2015)010, § 134.
[310] Voir également l'article 11 § 3 de la Convention 108+.
[311] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 275.
[312] Rapport de la FRA, section 1.2, avis 6.
[313] *Voir, par exemple*, CourEDH, *Big Brother Watch c. Royaume-Uni* [GC], précité, § 350 ; *Centrum för Rättvisa c. Suède* [GC], précité.
[314] *Voir la* section IV.E ci-dessus et le rapport de la FRA, cité ci-dessus, § 1.5.2.
[315] *Contrôle démocratique et efficace des services de sécurité nationaux*, précité, p. 45.
[316] Dans le contexte de la surveillance stratégique, *voir* Commission de Venise, CDL-AD(2015)011, précité, §§ 108-109.

se sont révélés plus efficaces dans plusieurs Etats, de même que la combinaison d'un organe spécialisé et d'un organe parlementaire.[317]

118. Lorsqu'un État n'a pas créé d'organe spécialisé dans le contrôle de la sécurité, les autorités chargées de la protection des données (APD) peuvent jouer un rôle important dans le système de contrôle de la sécurité et du renseignement dans son ensemble, en particulier en ce qui concerne les fichiers de sécurité (bien qu'il faille noter que de nombreuses APD n'ont pas le pouvoir d'enquêter sur les questions de sécurité nationale).[318]. Il est essentiel de doter les institutions de contrôle indépendantes de pouvoirs et de ressources humaines (y compris des professionnels spécialisés et techniquement qualifiés), financières et techniques suffisants, surtout si l'on considère les pouvoirs et les capacités étendus dont disposent généralement les services de renseignement et la nature secrète de bon nombre de leurs activités. Outre l'examen des rapports annuels, des enquêtes et des audits périodiques, les autorités chargées de la protection des données devraient être en mesure d'ouvrir des enquêtes à grande échelle ou ad hoc et d'avoir un accès permanent, complet et direct aux informations et aux documents classifiés afin de remplir leur mandat de manière efficace.

119. La Commission de Venise partage le point de vue de l'Agence des droits fondamentaux de l'UE selon lequel les organes de contrôle des services de renseignement devraient évoluer de la même manière que les lois sur le renseignement et les capacités des services de renseignement. L'accroissement des pouvoirs et des compétences de ces derniers doit être contrebalancé par un plus grand degré de contrôle indépendant, ainsi que par des ressources et une expertise adéquates pour garantir un contrôle efficace[319]. La coopération entre les autorités de contrôle concernées devrait garantir le contrôle « de bout en bout » préconisé par la CourEDH[320]. Il est important d'adopter une approche globale de la question du contrôle et de veiller à ce que les pouvoirs de contrôle prévus par la loi soient mis en œuvre dans la pratique.

H. Notification des mesures de surveillance ciblées

120. La CourEDH exige que la personne placée sous surveillance soit normalement informée a posteriori, afin qu'elle puisse être associée au contrôle de la mesure. Elle a donc établi une obligation générale de notification rétrospective, sous réserve d'exceptions[321]. Lorsqu'il n'existe pas de mécanisme permanent de plainte, l'absence totale d'obligation d'informer la personne interceptée à un moment donné après la fin de la surveillance a été jugée incompatible avec la Convention, car elle prive la personne interceptée de la possibilité de demander réparation pour les ingérences illégales dans ses droits au titre de l'article 8 et rend les recours disponibles en vertu du droit national théoriques et illusoires plutôt que pratiques et efficaces[322]. À l'inverse, la Cour a estimé que l'absence d'obligation de notifier à la personne concernée la mesure d'interception à tous les stades de son application était compatible avec la Convention, lorsque les personnes qui soupçonnaient que leurs communications faisaient ou avaient fait l'objet d'une interception pouvaient saisir un organisme de plainte indépendant, doté de pleins pouvoirs d'investigation, et dont la compétence n'était pas subordonnée à la notification de l'interception[323]. Bien qu'il ne soit pas possible d'exiger une notification dans tous les cas, il est souhaitable d'informer la personne visée par la surveillance dès que la notification peut être faite sans compromettre la finalité des mesures et après la levée des mesures de surveillance[324].

[317] Commission de Venise, CDL-AD(2015)010, précité, §§ 228-250.
[318] Rapport de la FRA, section 2.3.
[319] Rapport de la FRA, section 1.2, avis 3.
[320] CourEDH, *Segerstedt-Wiberg et autres c. Suède*, cité ci-dessus ; voir également le rapport de la FRA, section 3. Il convient également de noter que l'article 17 de la Convention 108+ exige une coopération obligatoire des autorités de contrôle dans les affaires transfrontalières.
[321] CourEDH, *Roman Zakharov c. Russie* [GC], précité, §§ 286 et ss.
[322] CourEDH, *Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev c. Bulgarie*, n° 62540/00, 28 juin 2007, §§ 90-91.
[323] CourEDH, *Kennedy c. Royaume-Uni*, précité, § 167.
[324] CourEDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, précité, § 238.

Dans un arrêt récent, s'appuyant *notamment* sur les conclusions d'un précédent avis de la Commission de Venise, la CourEDH a estimé que l'absence d'obligation de notification dans le contexte polonais de la surveillance secrète, même après un certain temps, était l'un des éléments permettant de conclure que le cadre juridique global était contraire à l'article 8 de la Convention[325].

121. Comme indiqué ci-dessus, la notification d'une cible individuelle peut évidemment compromettre des méthodes confidentielles ou des opérations en cours. Néanmoins, il est important de prévoir une obligation générale pour les autorités compétentes de notifier la cible *a posteriori* et de formuler des exceptions à cette règle. La décision, dans un cas particulier, de ne pas notifier une cible, même après la fin de la surveillance, doit toujours être notifiée à l'organe de contrôle externe et, normalement, approuvée par ce dernier. Lorsqu'il y a notification, et que la personne a donc connaissance de la surveillance, la procédure *ex parte* devant la juridiction qui a délivré le mandat de surveillance peut être complétée par une procédure pleinement contradictoire au cours de laquelle la juridiction examinera *de novo* la légalité de la surveillance. En effet, la notification est avant tout un mécanisme permettant d'obtenir réparation. La Commission de Venise a estimé qu'il est nécessaire que les personnes qui affirment avoir été lésées par les pouvoirs exceptionnels des agences de sécurité et de renseignement disposent d'une voie de recours[326].

122. L'article 13 de la CEDH exige des États qu'ils mettent en place un mécanisme de recours effectif pour les violations alléguées des droits de la Convention. De même, l'article 12 de la Convention 108+ exige des sanctions et des recours judiciaires et non judiciaires appropriés en cas de violation des dispositions de la Convention[327].

123. L'Agence des droits fondamentaux de l'Union européenne a souligné la nécessité de garantir des exigences minimales pour que les recours soient efficaces :[328] Tout d'abord, les organes non judiciaires doivent être indépendants ; en outre, ils doivent : (i) sensibiliser les individus aux mesures de surveillance, soit par la notification, soit par toute autre possibilité d'obtenir des informations sur les interceptions ; (ii) garantir l'accès des organes de recours aux informations classifiées ; (iii) garantir une réparation appropriée, par exemple la destruction des données collectées ou une réparation pécuniaire ; et (iv) garantir une expertise appropriée au sein des organes de recours.

I. Protection des tiers contre les mesures liées à l'utilisation de logiciels espions

124. L'une des particularités de l'utilisation des logiciels espions est que, selon les circonstances, elle peut se faire à distance (exécution de code à distance) ou physiquement (bien que cela soit vraisemblablement plus rare, car cela nécessite que la police ou l'agence de sécurité ait temporairement obtenu l'accès à l'appareil d'un suspect). L'exécution de code à distance a ceci de particulier que l'exploitation d'une vulnérabilité permettant à la police ou à l'agence de sécurité d'accéder à l'appareil du suspect risque d'aggraver les vulnérabilités logicielles et matérielles des appareils appartenant à des tiers[329]. Il s'agit là d'un équilibre difficile à trouver. D'une part, la

[325] *Ibidem*, §§ 238-247 ; *voir* Commission de Venise, CDL-AD(2016)012, *précité*. Des exigences similaires ont été imposées par la Cour de justice de l'Union européenne dans les affaires *Tele2 et Watson* et *Quadrature du Net*, précitées.

[326] Pour un aperçu des conclusions de la Commission de Venise sur les mécanismes de plainte*, voir* Commission de Venise, CDL-AD(2015)010, précité, §§ 251 et suivants.

[327] En ce qui concerne les autorités chargées de la protection des données, le rapport de la FRA, cité ci-dessus, section 2.3, donne un aperçu des pouvoirs de réparation des autorités chargées de la protection des données en Europe.

[328] Rapport de la FRA, section 2.1.

[329] L'autorité italienne de protection des données a souligné les risques pour la confidentialité dans le cas où l'inoculation d'un outil de surveillance intrusif n'est pas directe mais se fait par le téléchargement d'applications à partir de plates-formes librement accessibles à tout utilisateur. Dans ce cas, il existe un risque d'installation par des tiers qui n'ont aucun rapport avec les objectifs de l'enquête. Par conséquent, ce risque devrait être éliminé en

police ou l'agence de sécurité peut avoir de bonnes raisons de garder le silence sur une vulnérabilité donnée, qu'elle a trouvée ou créée, car cela lui permettra de l'exploiter à des fins d'enquête à l'avenir. D'autre part, le fait de laisser ces vulnérabilités ouvertes signifie que des acteurs malveillants, tels que des membres de groupes criminels organisés, etc. peuvent également les trouver et les exploiter. La législation devrait donc prévoir la protection des tiers contre l'exploitation, par les forces de l'ordre ou les services de renseignement, des vulnérabilités des logiciels. En outre, le forces de l'ordre ou les services de renseignement ne devraient pas laisser la sécurité du logiciel ou du matériel affecté dans un état généralement pire qu'avant le début de l'opération.

125. Dans un État, il a été suggéré que l'agence de police/sécurité mette en place un mécanisme permettant de peser correctement les avantages et les inconvénients du silence/de la divulgation dans chaque cas et de documenter sa prise de décision en la matière (pour permettre un contrôle futur et, le cas échéant, une obligation de rendre des comptes). En outre, il a été suggéré de prévoir un registre central des vulnérabilités pour chaque agence[330].

J. Obligation de détruire les « informations excédentaires »

126. Comme indiqué précédemment, l'utilisation de logiciels espions permet des mesures telles que la surveillance en temps réel des communications, des mouvements ou des activités en ligne, la recherche de données stockées sur l'appareil et l'activation d'une caméra et d'un microphone intégrés à des fins de surveillance. L'utilisation d'un logiciel espion sur un appareil mobile peut donc conduire à la collecte d'« informations excédentaires », c'est-à-dire d'informations non pertinentes pour l'enquête ou la surveillance particulière pour laquelle l'autorisation a été donnée. Cette collecte présente des risques particulièrement graves pour la vie privée et d'autres droits fondamentaux de la personne visée et de ses contacts, et soulève de sérieuses questions quant à la proportionnalité de l'utilisation d'un logiciel espion.

127. La CourEDH a constamment souligné la nécessité d'exiger la destruction immédiate de toutes les données qui ne sont pas pertinentes au regard de la finalité pour laquelle elles ont été obtenues[331]. Il est particulièrement important que de telles dispositions existent en ce qui concerne l'utilisation de logiciels espions en raison de la multiplicité des différents types d'informations, dont certaines sont des informations personnelles particulièrement sensibles, qui peuvent résulter de cette activité[332].

128. Deux types d'informations différentes peuvent émerger d'une enquête/surveillance, qui ne faisaient pas partie de la justification de la délivrance de l'autorisation d'utiliser un logiciel espion. La première est une information personnelle qui ne concerne pas une infraction ou une menace pour la sécurité nationale. Ces informations doivent être soumises à une obligation de destruction immédiate[333]. Cette obligation doit être assortie d'un contrôle[334]. Le deuxième type d'informations

autorisant uniquement l'utilisation d'applications qui empêchent l'acquisition par des tiers, ou en prévoyant que l'activité de capture ne doit commencer qu'après avoir vérifié que le logiciel est associé de manière unique au dispositif correspondant à celui couvert par le décret d'autorisation, *voir Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, précité, p. 43.

[330] Rapport d'examen 53 sur l'utilisation du pouvoir d'enquête en matière de piratage par l'AIVD et la MIVD en 2015, précité, p. 25.

[331] CourEDH, *Roman Zakharov c. Russie* [GC], précité, § 255, se référant à *Klass et autres c. Allemagne*, précité, § 52.

[332] La Cour constitutionnelle de la République de Moldova, dans son arrêt n° 31 du 23 septembre 2021, a estimé qu'il est nécessaire que la défense ait la possibilité d'accéder, soit à la fin de l'enquête pénale, soit à la fin du procès sur le fond, aux métadonnées obtenues à la suite de l'application de la surveillance secrète, même lorsque la destruction des informations obtenues par la surveillance secrète des métadonnées a été ordonnée parce qu'elle a été jugée non pertinente par le juge d'instruction.

[333] Voir par exemple l'article 23 de la loi suédoise (2020:62) sur la lecture des données secrètes.

[334] Il peut évidemment être difficile de concilier le contrôle et les exigences en matière de destruction, car si ces dernières fonctionnent correctement, l'organe de contrôle n'a rien à « surveiller ». Toutefois, il est possible de

est celui qui indique qu'une menace différente pour la sécurité nationale[335], ou un délit s'est produit, se produit ou se produira bientôt, c'est-à-dire une menace différente de celle pour laquelle l'autorisation a été accordée.

129. Pour éviter l'utilisation abusive des logiciels espions et maintenir la confiance du public dans le fait que le système n'est pas utilisé à mauvais escient, une règle raisonnable consiste généralement à exiger la destruction de ces informations. On peut envisager une exception lorsque l'infraction ou la menace pour la sécurité nationale en question, bien que ne faisant pas partie de la base de l'autorisation initiale, est néanmoins suffisamment grave (une menace réelle et sérieuse), si elle était connue à l'époque, pour remplir les conditions d'autorisation de l'utilisation d'un logiciel espion en premier lieu[336]. L'admission d'une telle exception présuppose une forme d'accès stratifié au matériel recueilli (voir note de bas de page 265 ci-dessus). En outre, pour éviter que cette exception ne devienne la règle dans la pratique, il devrait être obligatoire de demander et d'obtenir l'autorisation de conserver ces informations étroitement définies auprès du tribunal (ou de l'organe indépendant) qui a autorisé le mandat initial. Toutes ces autorisations devraient également être documentées et faire l'objet d'un contrôle externe.

K. Contrôle de l'exportation de logiciels espions

130. Comme indiqué ci-dessus, selon la résolution 2513(2023) de l'APCE, certains États membres du Conseil de l'Europe pourraient également avoir exporté Pegasus ou des logiciels espions similaires vers des pays tiers dotés de régimes oppressifs et autoritaires. Dans sa résolution 2045(2015), l'APCE a exhorté les États membres et observateurs à s'abstenir, *entre autres, d'*exporter des technologies de surveillance avancées vers des régimes autoritaires[337]. Le fait que les logiciels espions commerciaux soient développés par des entreprises privées est une question connexe. Comme l'ont montré les révélations de Pegasus, des entreprises privées ont été impliquées non seulement dans la production de logiciels espions, mais aussi dans la fourniture de logiciels espions en tant que service. À cet égard, l'externalisation de fonctions « essentielles » de l'État, telles que la surveillance, à des entreprises désireuses de vendre leurs services et de faire des bénéfices, en particulier dans un secteur privé non réglementé, comporte des risques très élevés d'utilisation abusive de ces technologies, en plus du risque lié à l'absence de responsabilité[338].

131. Les logiciels espions sont considérés comme des technologies à double usage (c'est-à-dire qu'ils peuvent être utilisés à des fins civiles et militaires), d'où la nécessité d'obtenir une licence d'exportation. Une bonne gestion de l'industrie des logiciels espions implique des contrôles efficaces des exportations. Le règlement (UE) 2021/821 a mis en place un régime de contrôle des exportations, du courtage, de l'assistance technique, du transit et du transfert de biens à double usage (le règlement sur les biens à double usage)[339]. Des règles globales ont été établies dans l'Arrangement de Wassenaar, auquel 31 États membres du Conseil de l'Europe sont parties[340]. L'Arrangement de Wassenaar a été conclu en 1999 en tant qu'accord multilatéral de

documenter le fait que des informations ont été détruites et la date à laquelle cela s'est produit. En outre, l'organe de contrôle peut vérifier que les exigences de destruction automatisée existantes fonctionnent, par exemple en les testant avec des informations hypothétiques.

[335] Cela suppose évidemment que les menaces pour la sécurité nationale puissent être spécifiées avec suffisamment de précision.

[336] *Voir* par exemple les articles 28 à 31 de la loi suédoise (2020:62) sur la lecture des données secrètes.

[337] APCE, Résolution 2045(2015), *Les opérations de surveillance massive*, 21 avril 2015, § 19.

[338] Voir, *mutatis mutandis*, Commission de Venise, CDL-AD(2009)038, *Rapport sur les entreprises militaires et de sécurité privées et sur l'érosion du monopole étatique du recours à la force*.

[339] Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union pour le contrôle des exportations, du courtage, de l'assistance technique, du transit et du transfert de biens à double usage (refonte).

[340] Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage. Les États participants à l'Arrangement de Wassenaar sont l'Afrique du Sud, l'Allemagne, l'Argentine, l'Australie, l'Autriche, la Belgique, la Bulgarie, le Canada, la Croatie, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Inde, l'Irlande, l'Italie, le Japon, la Lettonie, la

contrôle des exportations entre les États afin de contribuer à la sécurité et à la stabilité régionales et internationales, de promouvoir la transparence et une plus grande responsabilité dans les transferts d'armes conventionnelles et de biens et technologies à double usage. Toutefois, l'arrangement ne contient pas de lignes directrices ou de mesures d'application qui permettraient de lutter directement contre les violations des droits humains causées par les outils de surveillance[341].

132. La Commission de Venise estime que les Etats participant à l'Arrangement de Wassenaar pourraient étudier la possibilité de conditionner les règles d'octroi de licences technologiques au respect des normes en matière de droits humains par l'Etat destinataire (et la société productrice)[342]. En ce qui concerne les entreprises privées, l'octroi de licences d'exportation pourrait être subordonné à la mise en œuvre des principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme en ce qui concerne la conception, la vente, le transfert ou le soutien de ces technologies[343]. Cela est conforme aux recommandations pertinentes de l'APCE[344] et du Parlement européen[345] et suit également la ligne adoptée par les États participant à la Déclaration commune sur les efforts visant à contrer la prolifération et l'utilisation abusive des logiciels espions commerciaux (voir note de bas de page 249 ci-dessus). Les engagements pris dans cette déclaration pourraient être développés davantage en suivant les recommandations clés contenues dans le rapport 2019 du rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, qui sont, entre autres, les suivantes (i) établir un moratoire immédiat sur la vente et le transfert à l'échelle mondiale de technologies de surveillance privée jusqu'à ce que des garanties rigoureuses en matière de droits humains soient mises en place pour réglementer ces pratiques et garantir que les gouvernements et les acteurs non étatiques utilisent ces outils de manière légitime ;[346] et (ii) pour les entreprises, mettre en place des garanties solides afin de s'assurer que toute utilisation de leurs produits ou services est conforme aux normes en matière de droits humains. Ces garanties comprennent des clauses contractuelles qui interdisent la personnalisation, le ciblage, l'entretien ou toute autre utilisation qui viole le droit international des droits humains, des caractéristiques de conception technique pour signaler, prévenir ou atténuer les utilisations abusives, ainsi que des audits et des processus de vérification en matière de droits humains[347].

133. Conformément à l'engagement multigouvernemental mentionné aux paragraphes 73 et 132 ci-dessus et afin de promouvoir la transparence et un contrôle efficace, la Commission de Venise considère également que les gouvernements devraient, à titre de bonne pratique, faire des déclarations publiques annuelles indiquant s'ils ont acquis des licences pour des logiciels espions auprès de fournisseurs commerciaux et, le cas échéant, auprès de quelle entité commerciale[348].

Lituanie, le Luxembourg, Malte, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République de Corée, la République tchèque, la Roumanie, la Fédération de Russie, la Slovaquie, la Slovénie, la Suède, la Suisse, la Türkiye, l'Ukraine, le Royaume-Uni et les États-Unis.

[341] Rapport 2019 du RS des Nations Unies, cité ci-dessus, §§ 34-35.

[342] Comme le suggère Privacy International, l'octroi d'une licence pourrait être refusé lorsqu'il existe un « risque substantiel que ces exportations soient utilisées pour violer les droits humains, lorsqu'il n'existe pas de cadre juridique dans une destination régissant l'utilisation d'un élément de surveillance, ou lorsque le cadre juridique pour son utilisation n'est pas conforme à la législation ou aux normes internationales en matière de droits humains », *voir* D. Kaye, *The Spyware State and the prospects for accountability*, The Global Forum, Global Governance 27 (2021) Brill Nijhoff, pp. 487-488.

[343] Nations Unies, Représentant spécial du Secrétaire général chargé de la question des droits humains et des sociétés transnationales et autres entreprises, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies*. Voir également le Foreign, Commonwealth & Development Office du Royaume-Uni, *The Pall Mall Process : tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*, en particulier le paragraphe 8.

[344] APCE, Résolution 2513(2023), précitée, § 14.9.

[345] Recommandation du PE, précitée, § 56.

[346] Rapport 2019 du RS des Nations Unies, précité, § 66(a).

[347] *Ibidem,* § 67 (b).

[348] Des articles de presse récents concernant des litiges aux États-Unis suggèrent que les gouvernements pourraient dépendre des opérateurs commerciaux eux-mêmes pour effectuer une surveillance au moyen de logiciels espions.

Ils devraient également envisager toute autre mesure de transparence appropriée, telle que la publication de rapports réguliers sur l'utilisation de logiciels espions et sur les menaces posées par les logiciels espions commerciaux étrangers.

VI. Conclusion

134. Par lettre du 6 décembre 2023, le Président de l'Assemblée parlementaire du Conseil de l'Europe (APCE) de l'époque, M. Tiny Kox, a demandé à la Commission de Venise, conformément à la Résolution 2513 (2023) de l'Assemblée parlementaire sur « Pegasus et les logiciels espions similaires et la surveillance secrète de l'État », de mener une étude sur le cadre législatif et la pratique en matière de surveillance ciblée de tous les États membres (en priorité la Pologne, la Hongrie, la Grèce, l'Espagne et l'Azerbaïdjan ; puis l'Allemagne, la Belgique, le Luxembourg, les Pays-Bas et l'ensemble des autres États membres). En réponse à cette demande, la Commission de Venise a mené une étude comparative pour évaluer les règles existantes sur la surveillance ciblée et notamment sur l'utilisation de logiciels espions dans ses Etats membres. La Commission de Venise a examiné les dispositions juridiques des Etats qui ont envoyé des informations officielles à l'APCE et de ceux sur lesquels les membres de la Commission de Venise/experts ont fourni des informations en répondant à un questionnaire préparé par les rapporteurs. La complexité des cadres législatifs en question, le manque d'informations complètes et pratiques sur la mise en œuvre des normes internationales existantes, telles que l'article 9 de la Convention 108, ainsi que la rareté des réglementations spécifiques aux logiciels espions ont été des facteurs importants à prendre en compte lors de la préparation du rapport.

135. Les logiciels espions sont des outils de surveillance intrusifs qui peuvent être utilisés pour interférer avec des appareils électroniques, notamment des smartphones ou des ordinateurs, à l'insu de l'utilisateur, et qui permettent à l'opérateur de pénétrer dans les appareils et, selon l'outil spécifique, de suivre la géolocalisation en temps réel, de lire toutes les données stockées, toutes les communications effectuées (en contournant les protections possibles, telles que le cryptage) et de prendre le contrôle de tous les matériels et logiciels disponibles sur l'appareil, tels que les microphones ou les caméras. S'il n'est pas réglementé, le logiciel espion pourrait se transformer en un dispositif de surveillance 24 heures sur 24, avec un accès complet à tous les capteurs et à toutes les informations de l'appareil personnel. Cela en ferait une arme de surveillance qui pourrait être utilisée pour restreindre les droits humains, censurer et criminaliser la critique et la dissidence et harceler (voire supprimer) les journalistes, les militants des droits humains, les opposants politiques ou réprimer les organisations de la société civile, comme l'ont montré les multiples allégations et révélations. Il est donc essentiel de définir clairement les contours de l'utilisation des logiciels espions par les États afin de prévenir et d'éradiquer les pratiques abusives.

136. S'appuyant sur la jurisprudence de la CourEDH en matière de surveillance ciblée, sur les rapports précédents de la Commission de Venise, sur d'autres normes européennes et internationales telles que la Convention 108+ ainsi que sur l'analyse comparative de la législation pertinente dans les Etats membres de la Commission de Venise, le présent rapport a tenté d'identifier les garanties minimales qui devraient être mises en place, lorsqu'il s'agit de mesures intrusives de surveillance ciblée, afin d'éviter tout abus de pouvoir. En fin de compte, il appartiendra à la CourEDH, lorsqu'elle statuera sur les affaires de « logiciels espions » qui sont actuellement pendantes ou qui pourraient être portées devant elle, de fixer les normes spécifiques applicables dans ce domaine.

137. La Commission de Venise estime que l'utilisation et le développement de logiciels de surveillance intrusifs tels que les logiciels espions ne devraient être possibles que si le cadre juridique pertinent répond à certaines exigences strictes. Les garanties suivantes doivent au minimum être mises en place :

- Toutes les dispositions importantes régissant l'utilisation d'un outil de surveillance intrusif tel qu'un logiciel espion (le cas échéant) doivent être énoncées dans la législation primaire, qui devrait définir clairement le champ d'application (restreint) *ratione materiae, personae* et *temporis* de la surveillance ciblée au moyen d'un logiciel espion, qui ne peut être assimilé à d'autres mesures de surveillance ciblée ;
- En particulier, la législation devrait définir étroitement les cibles possibles des mesures de surveillance et prévoir que certaines catégories de personnes dont les interactions peuvent être protégées par le secret professionnel, ainsi que les journalistes, sont en principe exclus, avec certaines exceptions limitées ;
- La législation nationale doit établir une distinction claire entre le type d'enquête/de surveillance dans le cadre duquel l'utilisation d'un logiciel espion peut être autorisée et les données à caractère personnel qui peuvent être recherchées ; cette distinction devrait affecter l'évaluation de la nécessité et de la proportionnalité des mesures prises ;
- Les autorités requérantes (services répressifs ou services de renseignement) doivent toujours démontrer que les informations recherchées dans le cadre de l'enquête sont nécessaires à la réalisation du but légitime et qu'elles ne peuvent être obtenues par des moyens moins intrusifs ;
- Il doit exister des procédures d'autorisation ex ante bien réglementées devant un tribunal ou un autre organe indépendant (ou, dans des cas exceptionnels et urgents, des règles prévoyant la confirmation rapide de la mesure de surveillance ciblée par ce tribunal ou cet organe indépendant) ; et la durée des mesures de surveillance doit être limitée au strict nécessaire ;
- L'ensemble du processus de surveillance doit être soutenu par des institutions de contrôle externes indépendantes et efficaces, dotées de ressources suffisantes, qualifiées et spécialisées, et qui ne peuvent être confiées exclusivement à l'exécutif ;
- L'agence qui effectue l'enquête/surveillance autorisée et qui accède aux données ne doit pas accéder à plus de données que ne le permet l'autorisation qu'elle a reçue : toutes les données qui ne sont pas pertinentes au regard de la finalité pour laquelle elles ont été obtenues doivent être identifiées sans délai (excessif) et détruites de manière permanente ;
- Les personnes surveillées doivent être informées ultérieurement, sauf exceptions définies par la loi, afin qu'elles puissent être impliquées dans le contrôle et la contestation de la mesure ; lorsque cela n'est pas possible (par exemple, pour des questions de sécurité nationale), un mécanisme de plainte permanent doit être mis en place ;
- La législation devrait prévoir la protection des tiers contre l'exploitation, par les forces de l'ordre ou les services de renseignement, des vulnérabilités des logiciels ;
- Les États devraient conditionner les règles d'octroi de licences d'exportation de technologies au respect par l'État destinataire (et par la société productrice) des normes en matière de droits humains identifiées dans le présent rapport ;
- Les gouvernements devraient faire des déclarations publiques annuelles indiquant s'ils ont acquis des licences pour des logiciels espions auprès de fournisseurs commerciaux et, dans l'affirmative, auprès de quelle entité commerciale. Ils devraient également envisager toute autre mesure de transparence appropriée, telle que la publication de rapports réguliers sur l'utilisation de logiciels espions et sur les menaces posées par les logiciels espions commerciaux étrangers.

138. La Commission de Venise reste à la disposition de l'Assemblée parlementaire pour toute assistance supplémentaire dans ce domaine.