dirittifondamentali.it

La CEDU sulla normativa polacca in materia di sorveglianza segreta
(CEDU, sez. I, sent. 28 maggio 2024, ric. nn. 72038/17 e 25237/18)

La Corte Edu si pronuncia sui ricorsi presentati da cinque cittadini polacchi avverso la legislazione interna che autorizza un sistema di sorveglianza segreta e di conservazione dei dati delle telecomunicazioni, delle comunicazioni postali e digitali, al fine di un potenziale utilizzo da parte delle autorità nazionali competenti. Essi lamentavano l'assenza di rimedi ai sensi del diritto interno volti a consentire alle persone che credono di essere state sottoposte a sorveglianza segreta di ricorrere contro tale misura e farne verificare la legittimità.
I Giudici di Strasburgo hanno convenuto che la normativa nazionale non forniva garanzie sufficienti contro un ricorso eccessivo alla sorveglianza e l'ingerenza indebita nella vita privata delle persone; assenza di garanzie non sufficientemente controbilanciata dall'attuale meccanismo di controllo giurisdizionale.
Di qui la riconosciuta violazione del diritto al rispetto della vita privata e familiare e della corrispondenza.

***

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

PREMIÈRE SECTION

AFFAIRE XXXXX ET AUTRES c. POLOGNE

(Requêtes nos 72038/17 et 25237/18)

ARRÊT

STRASBOURG

28 mai 2024

Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 de la Convention. Il peut subir des retouches de forme.

En l'affaire XXXXX et autres c. Pologne,

La Cour européenne des droits de l'homme (première section), siégeant en une chambre composée de :

Marko Bošnjak, *président*,
Péter Paczolay,
Krzysztof Wojtyczek,
Erik Wennerström,
Raffaele Sabato,
Lorraine Schembri Orland,
Ioannis Ktistakis, *juges*,
et de Ilse Freiwirth, *greffière de section*,

Après en avoir délibéré en chambre du conseil le 11 avril 2024,

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

INTRODUCTION

1. L'affaire concerne, sous l'angle des exigences de l'article 8 de la Convention, la législation nationale autorisant un système de surveillance secrète (le contrôle opérationnel ainsi que la conservation des données de communications téléphoniques, postales et électroniques (« les données de communication ») aux fins d'un accès éventuel par les autorités nationales compétentes). Elle porte en particulier sur la question de l'existence en droit interne d'un recours permettant aux personnes pensant avoir fait l'objet d'une surveillance secrète de s'en plaindre et d'en contester la légalité (l'article 13 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention ») combiné avec l'article 8 de celle-ci).

PROCÉDURE

2. À l'origine de l'affaire se trouvent deux requêtes (nos 72038/17 et 25237/18) dirigées contre la République de Pologne et dont cinq ressortissants de cet État, MM. Mikołaj Pietrzak et Wojciech Klicki et Mmes Dominika Bychawska-Siniarska, Barbara Grabowska-Moroz et Katarzyna Szymielewicz (« les requérants ») ont saisi la Cour en vertu de l'article 34 de la Convention le 29 septembre 2017 et le 12 février 2018, selon le cas.

3. Les requérants ont été représentés par Mme Małgorzata Mączka-Pacholak, avocate. Le gouvernement polonais (« le Gouvernement ») a été représenté par son agent, M. Jan Sobczak, du ministère des Affaires étrangères.

4. Le 27 septembre 2019, les requêtes ont été communiquées au Gouvernement.

5. L'autorisation de se porter tiers intervenant a été accordée aux organismes suivants : l'European Criminal Bar Association (l'« ECBA »), Privacy International, Article 19, Electronic Frontier Foundation, Fair Trials, l'association ePaństwo, le Conseil national des barreaux polonais (l'« NRA »), les Rapporteurs spéciaux des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste et sur la protection et la promotion de la liberté d'expression, le Commissaire aux droits de l'homme de la République de Pologne et la Commission internationale de juristes (la « CIJ »).

6. Tant les requérants que le Gouvernement ont déposé des observations écrites sur le fond de l'affaire (article 59 § 1 du règlement). La Cour a reçu en outre des commentaires des tiers intervenants.

7. Le 10 mai 2022, la chambre de la première section à laquelle l'affaire avait été attribuée a décidé de tenir une audience. Celle-ci s'est déroulée en public au Palais des droits de l'homme à Strasbourg, le 27 septembre 2022.

Ont comparu :
– pour le Gouvernement
M. Jan Sobczak, agent du Gouvernement,
Mme Marta Bielińska, ministère des Affaires étrangères, conseillère,
M. Konrad Malinowski, cabinet du Premier ministre, conseiller,
Mme Edyta Gołąb, Bureau central de la police nationale, conseillère,
MM. Tomasz Książkiewicz, Bureau central de la police nationale, conseiller,
M. Arkadiusz Matyjasik, police des frontières, conseiller ;

– pour les requérants
Mme Małgorzata Mączka-Pacholak, conseil,
M. Mikołaj Pietrzak,
Mmes Dominika Bychawska-Siniarska et Barbara Grabowska-Moroz,
M. Wojciech Klicki, requérants ;

– pour le Commissaire aux droits de l'homme de la République de Pologne, tiers intervenant
M. Mirosław Wróblewski, directeur, Bureau du Commissaire,
Mme Kinga Zielińska, expert en chef, Bureau du Commissaire ;

- pour l'ECBA, tiers intervenant
M. Andreas Alexios Anagnostakis, spécialiste des droits de l'homme ;

- pour le Rapporteur spécial des Nations Unis sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, tiers intervenant
Mmes Anne Charbord, conseillère juridique principale, et Karen Lorena Reyes Tolosa, spécialiste des droits de l'homme.

8. La Cour a entendu M. Sobczak, Mmes Mączka-Pacholak et Grabowska-Moroz et M. Pietrzak en leurs déclarations et en leurs réponses aux questions posées par le président et par les juges Wennerström, Wojtyczek, Sabato, Ktistakis, Schembri Orland, Derenčinović et Bošnjak. Mme Charbord, M. Wróblewski, Mme Zielińska et M. Anagnostakis ont également fait des déclarations.

EN FAIT

I. LE CONTEXTE

9. Les 15 janvier et 10 juin 2016, le Parlement polonais adopta respectivement une loi portant modification de la loi sur la police et de certaines autres dispositions législatives (*Ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw* - « la loi du 15 janvier 2016 ») et une loi relative à la lutte

contre le terrorisme ((*Ustawa o działaniach antyterrorystycznych* - « la loi anti-terrorisme » (paragraphes 51-57 ci-dessous)).

10. Lesdites lois furent critiquées notamment par le Commissaire aux droits de l'homme polonais (« le Commissaire aux droits de l'homme »), l'Inspecteur général sur la protection des données, le Conseil national de la Justice, le conseil national des barreaux et par des députés d'opposition. Plusieurs organisations de la société civile ayant une expertise en la matière considéraient que la nouvelle législation, sous couvert de mettre en œuvre l'arrêt K 23/11 de la Cour constitutionnelle (paragraphe 73 ci-dessous), renforçait les pouvoirs de surveillance des autorités dans de nombreux domaines et qu'elle était incompatible avec certaines des obligations internationales de la Pologne relatives aux droits de l'homme. Dans son avis CDL-AD (2016) 012 du 13 juin 2016 (paragraphe 92 ci-dessous), la Commission de Venise exprima des réserves à l'égard de la loi du 15 janvier 2016.

II. LES CIRCONSTANCES DE L'ESPÈCE

11. Les requérants sont nés respectivement en 1973, 1982, 1987, 1981 et 1986 et résident à Varsovie. Le requérant Mikołaj Pietrzak est avocat et ancien chef de l'ordre des avocats du barreau de Varsovie. Les autres requérants sont des salariés d'organisations non gouvernementales (ONG) basées à Varsovie ; la requérante Barbara Grabowska-Moroz est enseignante-chercheuse à l'université et experte externe de la Fondation Helsinki pour les droits de l'homme, et la requérante Dominika Bychawska-Siniarska est membre de cette même Fondation. Le requérant Wojciech Klicki et la requérante Katarzyna Szymielewicz sont membres de la fondation Panoptykon.

A. Les demandes d'accès à l'information publique formulées par le requérant Klicki et la requérante Szymielewicz

12. Le 14 mars 2016, se prévalant des dispositions de l'article 2 de la loi sur l'accès à l'information publique (*Ustawa o dostępie do informacji publicznej*, paragraphe 59 ci-dessous), le requérant Klicki et la requérante Szymielewicz invitèrent le chef de l'Agence nationale de la sécurité (*Agencja Bezpieczeństwa Wewnętrznego* - « l'ABW ») à leur indiquer si, au cours de la période comprise entre le 1er janvier 2012 et le 29 février 2016, ils avaient fait l'objet d'une surveillance secrète de la part des services relevant de sa supervision, et si lesdits services avaient ou non collecté à leur insu des données liées à leurs télécommunications.

13. Le 31 mars 2016, le chef de l'ABW rejeta les demandes formées par les deux requérants. Renvoyant aux dispositions de la loi sur l'Agence nationale de la sécurité et les services de renseignement (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* - « la loi sur l'ABW et les services de renseignement »), qui selon lui étaient pertinentes en l'espèce, il considéra que bien que l'information dont les intéressés avaient sollicité la communication fût considérée comme « publique », au sens de l'article 1 de la loi sur l'accès à l'information publique, elle ne pouvait leur être communiquée pour des raisons qui étaient énoncées dans la loi du 5 août 2010 sur la protection des données classées (*Ustawa o ochronie informacji niejawnych*, paragraphe 60 ci-dessous). Il indiqua en outre, d'une part, que les mesures de contrôle opérationnel

auxquelles les services de l'ABW avaient recours étaient confidentielles et, d'autre part, que la mise en œuvre par les agents des services concernés des mesures en question ne nécessitait aucunement l'accord des personnes visées et s'effectuait sans que celles-ci en fussent informées. Il précisa également que les registres dans lesquels les éléments obtenus dans le cadre des mesures susvisées étaient consignés étaient confidentiels et que seul pouvait être rendu public le nombre d'individus ayant fait l'objet, selon le rapport que le procureur en chef du parquet national soumettait annuellement au Parlement, d'une surveillance au cours d'une période de référence. Il expliqua qu'en vertu de l'article 39 de loi sur l'ABW, seuls les tribunaux et les procureurs compétents pouvaient accéder, sous certaines conditions et sous réserve de son accord, en sa qualité de chef de l'ABW, aux informations issues des mesures de surveillance et que, par ailleurs, les documents relatifs au contrôle opérationnel étaient transmis au Premier ministre selon des modalités respectueuses des dispositions relatives à la protection des données classées. Il ajouta que les informations dont les requérants réclamaient la communication avaient été traitées conformément aux prescriptions de l'article 3 § 1 de la loi sur l'accès à l'information publique et que, par conséquent, elles ne pouvaient être divulguées aux intéressés qu'en cas d'impératif d'intérêt général.

14. Le 31 mars 2016, le chef de l'ABW rejeta une demande analogue qui lui avait été adressée par la requérante Szymielewicz.

15. Le 6 mai 2016, le chef de l'ABW rejeta la demande de réexamen de dossier qui avait été déposée par le requérant Klicki. Il considéra que les principes dégagés dans la jurisprudence pertinente des juridictions administratives ne lui permettaient pas de souscrire aux arguments de l'intéressé selon lesquels celui-ci aurait bénéficié d'un droit d'accès étendu aux informations dont il sollicitait la communication. En marge de sa décision, il précisa que celle-ci était susceptible de recours devant le tribunal administratif.

B. Les plaintes formulées par les requérants sur le fondement de l'article 227 du code de procédure administrative (« le CPA »)

16. Entre juin et juillet 2017, chacun des requérants saisit, sur le fondement de l'article 227 du CPA (paragraphe 67 ci-dessous), le Premier ministre et les responsables respectifs de différents services de police et de renseignement – parmi lesquels l'ABW, le Bureau central de lutte contre la corruption (*Centralne Biuro Antykorupcyjne* - « le CBA »), le service de contrôle fiscal (*Krajowa Administracja Skarbowa* - « le KAS »), les services de contre-espionnage militaire (*Służba Kontrwywiadu Wojskowego* - « le SKW »), la police nationale, la police des frontières (*Straż Graniczna* - « la SG ») et la police militaire (*Żandarmeria Wojskowa* - « la ŻW ») – de plaintes portant sur certaines dispositions de la législation nationale relative à la surveillance secrète. Dans le cadre desdites plaintes, les requérants critiquaient plus particulièrement la législation litigieuse en ce que, selon eux, elle permettait aux agents des services en question de surveiller leurs télécommunications et de collecter, à leur insu, les informations les concernant telles que visées à l'article 180 c et d de la loi du 16 juillet 2004 sur les télécommunications (*Ustawa Prawo telekomunikacyjne*, paragraphe 61 ci-dessous) et à l'article 18 §§ 1-5 de la loi du 18 juillet 2002 sur la prestation de services en ligne (*Ustawa o świadczeniu usług drogą elektroniczną*, paragraphe 63 ci-dessous). Ils estimaient qu'eu égard à leurs activités professionnelles et publiques respectives, il était très probable qu'une telle surveillance ait

été mise en place à leur endroit. Ils ajoutaient que les agents des services en question n'étaient pas tenus de les informer d'un éventuel recours à pareille mesure les concernant, y compris après sa cessation, et arguaient qu'un tel défaut d'information était contraire à l'article 51 §§ 3 et 4 de la Constitution (paragraphe 26 ci-dessous) et qu'il avait pour conséquence de les empêcher de faire contrôler la légalité de la surveillance par un tribunal. Les intéressés soutenaient que ledit défaut de notification des mesures de surveillance secrète aux individus visés, combiné avec une absence de contrôle effectif de celles-ci et avec des insuffisances de la législation nationale y afférente, était contraire au principe de l'État de droit en démocratie et portait atteinte à leurs intérêts légitimes.

17. Entre juin et septembre 2017, les responsables des services de police et de renseignement susmentionnés répondirent aux plaintes respectives des requérants.

18. Le chef de l'ABW indiqua aux intéressés que les informations relatives à la surveillance secrète d'individus étaient confidentielles et protégées en application des dispositions pertinentes de la loi sur l'ABW et les services de renseignement et de la loi sur la protection des données classées. Il précisa qu'en tant qu'institution respectueuse de la loi, l'ABW ne pouvait pas communiquer aux requérants d'informations sur ce point, ni répondre à leur question quant à l'existence ou non de mesures de surveillance les concernant. Il ajouta que la mise en œuvre de mesures de surveillance secrète par les agents soumis à sa supervision était contrôlée par le parquet et les tribunaux compétents.

19. Pour sa part, le chef du CBA expliqua aux requérants qu'en application des dispositions pertinentes de la Constitution et de la loi sur le CBA (*Ustawa o Centralnym Biurze Antykorupcyjnym*), les mesures opérationnelles d'investigation étaient diligentées par les agents placés sous sa supervision, et que la personne qui en faisait l'objet n'en était pas informée, sauf dans le cas où les renseignements obtenus au moyen desdites mesures étaient utilisés ultérieurement en tant qu'éléments de preuve dans une procédure pénale dirigée contre elle. Il précisa qu'à supposer même que les requérants eussent été visés par des mesures de ce type, le recours à celles-ci aurait nécessairement été décidé dans le respect des procédures prévues à cette fin par la législation pertinente. Il releva qu'une éventuelle surveillance des communications du premier requérant aurait été en outre soumise au régime de protection renforcée prévu par l'article 18 de la loi sur le CBA relativement au secret professionnel des avocats. Il ajouta, à cet égard, que rien dans la législation nationale n'empêchait les agents du CBA de mettre en place des mesures de surveillance à l'endroit des avocats.

20. De son côté, le commandant en chef de la ŻW informa les requérants que les agents placés sous sa supervision pouvaient en théorie engager des mesures opérationnelles d'investigation à leur égard si les conditions prévues à cette fin par la législation pertinente en la matière étaient réunies. Il observa que les affirmations des requérants quant à l'existence supposée de pareilles mesures les concernant n'avaient pas été prouvées et que leur vraisemblance même n'était pas établie. Il ajouta qu'en application de la législation en cause, dont la constitutionnalité n'avait, selon lui, encore jamais été remise en question, la police militaire n'avait pas compétence pour notifier les mesures de surveillance secrète aux individus visés, y compris après la levée de celles-ci. Il souligna en outre que la collecte par les agents relevant de sa supervision des données liées aux communications téléphoniques, aux communications postales et aux communications numériques surveillées était soumise au contrôle du tribunal régional des armées compétent.

21. Quant au commandant en chef de la SG , il indiqua aux requérants que la législation nationale pertinente ne prévoyait en principe aucune obligation pour ses services d'informer les individus concernés des mesures appliquées à leur endroit en matière de reconnaissance, de recherche et de collecte de données liées aux télécommunications, aux communications numériques et aux communications postales, excepté dans le cas mentionné à l'article 10 c alinéa 9 de la loi du 12 octobre 1990 sur la police des frontières (*Ustawa o Straży Granicznej*). Il ajouta que la personne faisant l'objet de la surveillance secrète n'était avisée de celle-ci qu'en cas d'utilisation, dans le cadre d'une procédure pénale dans laquelle elle avait le statut de partie, des informations ainsi obtenues. Il précisa en outre que les mesures de surveillance secrète étaient diligentées par les agents soumis à sa supervision uniquement en vue de la prévention des infractions visées aux articles 9 e § 1 alinéa 1-9 e de la loi sur la SG, de la découverte des auteurs de ces infractions et de la collecte des données mentionnées à l'article 10 b § 1 de la même loi. Il signala également que la mise en place de cette surveillance par les agents de la SG était contrôlée par le parquet et les tribunaux compétents.

22. Le chef du SKW, quant à lui, fit savoir aux requérants que l'application des mesures de collecte de données indiquées à l'article 32 alinéa 1 de la loi du 9 juin 2006 sur le SKW et le service de renseignement militaire (*Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego)* ne pouvait faire l'objet de contestations sur le fondement de l'article 227 du CPA, mais qu'elle était néanmoins soumise au contrôle du tribunal régional des armées de Varsovie en vertu des dispositions pertinentes de l'article 32 a de la même loi.

23. De leur côté, les services du bureau central de la police nationale confirmèrent que les agents de police pouvaient engager des mesures de surveillance secrète dans les cas précisément visés par la loi sur la police et dans le respect des exigences de celle-ci. Relevant que dans leurs plaintes respectives, les intéressés avaient interrogé le commandant en chef de la police nationale sur le point de savoir si une surveillance secrète avait été mise en place par les agents de police à leur endroit, ils estimèrent ne pas être en mesure de répondre à cette question eu égard au caractère selon eux hypothétique et insuffisamment précis de celle-ci.

24. Pour sa part, le responsable du KAS informa les requérants que les mesures opérationnelles d'enquête étaient confidentielles, que les individus visés par celles-ci ne pouvaient se plaindre de leur application sauf dans les situations indiquées à l'article 117 § 3 de la loi du 16 novembre 2016 sur le KAS (*Ustawa o Krajowej Administracji Skarbowej*), et que par conséquent les agents du KAS procédaient à la collecte et au traitement des informations issues des mesures en cause sans en aviser la personne concernée et sans solliciter son accord. Il précisa qu'il découlait des dispositions pertinentes de ladite loi que l'application de mesures opérationnelles d'enquête à l'égard d'un individu ne dépendait aucunement de l'activité professionnelle ou publique de celui-ci. Il rappela que le droit énoncé à l'article 51 § 3 de la Constitution (paragraphe 26 ci-dessous) pouvait faire l'objet de restrictions prévues par la loi, telle, en l'occurrence, la loi sur le KAS. Il ajouta que les dispositions pertinentes précisaient suffisamment les circonstances dans lesquelles une surveillance pouvait être engagée par les agents soumis à sa supervision.

25. Enfin, les services compétents du cabinet du Premier ministre indiquèrent aux requérants que, selon leur responsable, les chefs des différents services de police et de renseignement avaient amplement répondu à leurs interrogations à propos d'une hypothétique surveillance les concernant. Ils précisèrent que, dans le cadre de la mise en œuvre de leurs missions respectives, les services

spéciaux de l'État recouraient aux mesures de surveillance secrète prévues par la législation pertinente, et que les moyens et méthodes qu'ils utilisaient à cette fin étaient confidentiels et protégés en vertu des lois régissant les services concernés et de la loi sur la protection des données confidentielles.

LE CADRE JURIDIQUE ET LA PRATIQUE PERTINENTS

I. LE CADRE JURIDIQUE ET LA PRATIQUE INTERNES PERTINENTS

A. La Constitution

26. La Constitution de la République de Pologne se lit ainsi en ses dispositions pertinentes en l'espèce :

Article 31

« (...)

3. L'exercice des libertés et des droits constitutionnels ne peut faire l'objet que des seules restrictions prévues par la loi lorsqu'elles sont nécessaires, dans un État démocratique, à la sécurité ou à l'ordre public, à la protection de l'environnement, de la santé et de la moralité publiques ou des libertés et des droits d'autrui. Ces restrictions ne peuvent porter atteinte à l'essence des libertés et des droits. »

Article 47

« Chacun a droit à la protection juridique de la vie privée et familiale, de sa dignité et de sa réputation, et [le droit] de décider de sa vie personnelle. »

Article 51

« 1. Nul ne peut être obligé, autrement qu'en vertu d'une loi, de révéler des informations le concernant.

2. Les pouvoirs publics ne peuvent recueillir, assembler et rendre accessibles d'autres informations sur les citoyens que celles qui sont nécessaires dans un État démocratique de droit.

3. Chacun a droit à l'accès aux documents officiels qui le concernent et aux bases de données. Les restrictions à ce droit ne peuvent être prévues que par la loi.

4. Chacun a le droit d'exiger la rectification et l'élimination d'informations fausses, incomplètes ou recueillies de façon contraire à la loi.

5. Les principes et la procédure du recueil et de l'accès à l'information sont prévus par la loi. »

Article 61

« 1. Le citoyen a le droit d'obtenir des informations sur l'activité des pouvoirs publics et sur les personnes exerçant des fonctions publiques. Ce droit implique également l'obtention

d'informations sur les activités des organes d'autogestion économiques et professionnels ainsi que [sur celles] des personnes et des organisations lorsque celles-ci accomplissent des missions de puissance publique et gèrent des biens appartenant aux communes ou à l'État.

2. Le droit d'obtenir des informations implique aussi le droit d'accès aux documents et aux réunions des organes de la puissance publique élus au suffrage universel, y compris l'enregistrement du son ou de l'image.

3. Les droits mentionnés aux premier et deuxième alinéas ne peuvent être l'objet de restrictions que si elles sont nécessaires à la protection des libertés et droits d'autres personnes et entités économiques, à la protection de l'ordre public, de la sécurité ou d'un intérêt économique important de l'État.

4. Les modalités de communication des informations visées aux premier et deuxième alinéas sont prévues par la loi, et, pour la Diète et le Sénat, par leurs règlements intérieurs. »

Article 79

« 1. Toute personne dont les libertés ou les droits ont été violés a le droit, conformément aux principes définis par la loi, de porter plainte devant la Cour constitutionnelle relativement à la conformité à la Constitution de la loi ou de tout autre acte normatif en vertu duquel l'autorité judiciaire ou l'administration publique se sont définitivement prononcées sur les libertés ou les droits de cette personne ou sur ses devoirs tels que définis par la Constitution. »

B. Le cadre juridique national relatif à la surveillance secrète en vigueur à l'époque des faits

27. Le cadre juridique polonais relatif à la surveillance secrète est constitué de plusieurs lois, parmi lesquelles celles portant règlementation des activités respectives des différents services de police et de renseignement[1]. L'ensemble des textes pertinents prévoient un modèle de surveillance quasi analogue, la loi sur la police servant d'exemple *mutatis mutandis* pour les autres organismes.

28. L'article 19 de la loi sur la police contient les règles relatives au contrôle opérationnel (désignée par la notion d'operational control dans la traduction anglaise officielle de la loi sur la police ; voir, paragraphes 31-44 ci-dessous) et l'article 20 c de la même loi traite des données de communication (voir, paragraphes 45-50 ci-dessous). Le contrôle opérationnel précède fréquemment, pour la justifier, l'ouverture d'une enquête pénale, mais ne donne pas toujours lieu à l'engagement d'une procédure pénale (*kontrola pozaprocesowa*). Les informations obtenues par ce moyen peuvent être présentées ultérieurement comme éléments de preuve dans le cadre de poursuites pénales. Les mesures de surveillance diligentées au cours d'une procédure pénale *(kontrola procesowa*) sont régies par les dispositions pertinentes du code de procédure pénale (« le CPP ») (paragraphe 58 ci-dessous).

29. De manière générale, la surveillance secrète est exercée au titre de la répression des infractions et le renseignement est mené dans un but de sécurité nationale. Les finalités que peuvent poursuivre les mesures de surveillance diligentées par les différents services de police et de renseignement sont précisées dans les lois portant réglementation de leurs missions respectives.

30. En matière de surveillance secrète, la législation nationale prévoit deux régimes juridiques distincts : l'un concerne le contrôle opérationnel et l'autre régit la conservation et le traitement des données de communication. Ces deux modes de surveillance diffèrent quant aux motifs pour lesquels ils sont ordonnés et aux règles de procédure qui leur sont applicables.

1. Le contrôle opérationnel

31. Selon le paragraphe 6 de l'article 19 de la loi sur la police, relèvent du contrôle opérationnel les mesures telles que les écoutes, l'enregistrement du contenu de conversations téléphoniques ou de correspondances effectuées *via* les réseaux de télécommunications et de communications numériques (e-mails, messageries, etc.) ainsi, entre autres, les enregistrements sonores, la prise d'images de lieux et de moyens de transport privés, l'enregistrement de données inscrites sur des supports informatiques, des dispositifs de télécommunication ou des systèmes informatiques et téléinformatiques et le contrôle de colis postaux. Ce mode de surveillance permet à la police de connaître la teneur de communications passées entre des interlocuteurs qui pensent échanger de manière confidentielle.

32. L'article 19 § 1 de la loi sur la police comporte une liste exhaustive des infractions pouvant donner lieu à des mesures de contrôle opérationnel. Cette disposition précise en outre que le contrôle opérationnel peut être ordonné à l'occasion de l'application par la police de mesures opérationnelles d'enquête aux fins de la prévention ou de la découverte des infractions visées, de la découverte des auteurs de ces infractions et de la collecte et de l'enregistrement d'éléments de preuve dès lors que d'autres moyens paraissent inefficaces ou inutiles.

33. Selon l'article 19 §§ 1, 1a, 2 et 7 de la même loi, le contrôle opérationnel peut être ordonné par le tribunal compétent, qui statue alors sur une demande écrite formée par un responsable, habilité à cette fin, du service de police et de renseignement concerné (à savoir le commandant en chef de la police nationale ou celui de la police régionale) et préalablement approuvée par le procureur compétent (à savoir le procureur en chef du parquet national ou le procureur régional). La demande de mise en place d'un contrôle opérationnel doit être étayée. Elle doit indiquer en particulier le numéro du dossier ou son cryptonyme, les éléments factuels se rapportant à une infraction avec, si possible, leur qualification juridique, les circonstances justifiant le recours à un contrôle opérationnel, y compris celles montrant que d'autres moyens seraient inefficaces ou inadéquats, les éléments permettant de clairement identifier l'objet du contrôle opérationnel ainsi que l'endroit où il aura lieu et les moyens avec lesquels il sera réalisé, ainsi que l'objectif, la durée d'application et le type de contrôle opérationnel dont il s'agit.

34. Selon l'article 19 § 8 de ladite loi, la surveillance est autorisée pour une période n'excédant pas trois mois. Une prolongation peut être ordonnée par une décision de justice, à la demande du service compétent et sur autorisation écrite du procureur, pour une période supplémentaire d'un maximum de trois mois si les motifs initiaux de la mise en place de la surveillance sont encore valables. Dans les cas dûment justifiés (si la survenance de faits nouveaux impose une action aux fins de la prévention ou de la détection d'une activité criminelle, ou de la recherche des personnes se livrant à une telle activité et de la collecte d'éléments de preuve), la surveillance peut être prolongée par une juridiction supérieure pour plusieurs périodes consécutives fixées par ladite juridiction, pour une durée maximale globale de douze mois. Au total, la durée de la surveillance

ne peut excéder dix-huit mois. Le tribunal statuant sur la demande de prolongation du contrôle opérationnel examine les éléments présentés à l'appui de celle-ci, y compris ceux déjà recueillis au moyen dudit contrôle.

35. L'article 19 § 3 de la même loi dispose qu'exceptionnellement, en cas d'extrême urgence et, tout particulièrement, de risque de perte d'information ou d'altération des éléments de preuve, la police peut procéder sans autorisation à la surveillance secrète, celle-ci devant être interrompue si l'autorisation judiciaire n'est pas obtenue dans les cinq jours suivant le début de l'application de la mesure. Dans ce dernier cas, les informations recueillies durant ce délai au moyen du contrôle doivent être détruites par une commission protocolaire.

36. Selon l'article 19 § 11 de ladite loi, le tribunal qui examine la demande de contrôle opérationnel statue à juge unique. Celui-ci accomplit les différents actes de procédure dans des conditions similaires à celles prévues pour le transfert, la conservation et la divulgation des informations classifiées et en prenant en compte, de manière appropriée, les dispositions émises sur le fondement de l'article 181 § 2 du code de procédure pénale (« le CPP »). Seuls le procureur et le représentant de l'autorité demanderesse participent à la séance, tenue à huis-clos, du tribunal.

37. L'article 19 § 12 de la même loi impose aux sociétés de télécommunication, aux opérateurs postaux et aux prestataires de services fournis par voie électronique l'obligation d'assurer à leurs frais les conditions techniques et organisationnelles rendant possible la mise en œuvre du contrôle opérationnel par la police.

38. L'article 19 §§ 13 et 14 de cette loi prévoit que le contrôle opérationnel doit prendre fin dès que les raisons qui ont justifié sa mise en place ont cessé d'exister et au plus tard à l'expiration de la période pour laquelle il a été autorisé. Après la levée du contrôle opérationnel, l'autorité de police visée au paragraphe 1 de l'article 19 informe le procureur compétent des éléments qui en sont ressortis et, en cas de demande faite en ce sens par ledit procureur, de la manière dont la surveillance a été conduite.

39. Selon l'article 19 § 15 de la loi en question, en cas de recueil, par les autorités, d'éléments de preuve rendant possible l'ouverture d'une procédure pénale ou s'avérant pertinents à l'égard de poursuites pénales en cours, l'autorité compétente (à savoir le commandant en chef de la police nationale, celui du Bureau central d'investigation ou celui de la police départementale) transmet au procureur visé au paragraphe 1 de la disposition l'ensemble des éléments qui ont été obtenus dans le cadre des mesures opérationnelles d'investigation. Les dispositions de l'article 393 § 1 § 1 du CPP (paragraphe 58 ci-dessous) s'appliquent *mutatis mutandis* à la procédure menée devant le tribunal relativement à ces éléments.

40. L'article 19 § 15 de la même loi indique la procédure à suivre concernant les informations couvertes par le secret professionnel. Les fonctionnaires de police compétents doivent détruire les informations qui relèvent de la protection du secret professionnel absolu dont jouissent les avocats de la défense et les prêtres (article 19 § 15 f, point 1 de la loi sur la police, lu en combinaison avec l'article 178 du CPP), et transmettre au procureur, puis au tribunal, les éléments recueillis bénéficiant d'une protection moindre au titre du secret professionnel, comme c'est le cas du secret professionnel prévu pour les notaires, les avocats et les conseillers juridiques (sauf s'ils agissent en tant qu'avocats de la défense), les conseillers fiscaux, les médecins, les médiateurs et les journalistes (articles 19 §§ 15 f, alinéa 2 et 15 g de la loi lu en combinaison avec les articles 178 a et 180 §§ 2 et 3 du CPP). Le

tribunal statue sans délai et peut soit autoriser l'utilisation des informations dans une procédure pénale, s'il estime que l'intérêt de la bonne administration de la justice l'exige et qu'un fait pertinent ne peut pas être établi au moyen d'une autre preuve, soit, dans le cas contraire, ordonner leur destruction. La décision du tribunal ordonnant la destruction d'informations obtenues au moyen d'un contrôle opérationnel peut être contestée par la voie d'un recours ouvert au seul procureur. L'autorité de police concernée est tenue de se conformer à l'ordre de destruction du tribunal concernant les éléments visés au paragraphe 15 h et doit ordonner leur destruction sans délai par une commission protocolaire. Elle informe en outre immédiatement le procureur visé à l'article 19 § 15 g de la destruction des éléments en question.

41. L'article 19 § 16 de la loi en question énonce que la personne visée par le contrôle opérationnel ne peut avoir accès aux informations recueillies au cours de ce contrôle.

42. Selon l'article 19 § 17 de ladite loi, les éléments qui ont été obtenus au moyen d'un contrôle opérationnel et qui n'ont pas donné lieu à des poursuites sont détruits sans délai par une commission protocolaire.[2] Ladite suppression est effectuée sur décision de l'autorité de police ayant sollicité l'autorisation de mise en œuvre de la mesure en question.

43. Le procureur national, le tribunal, le procureur et l'autorité de police compétents consignent les demandes et décisions relatives au contrôle opérationnel dans des registres dédiés. Un registre central est également tenu par le commandant en chef de la police nationale. Les registres en question sont établis sous forme électronique, sous réserve de dispositions contraires relatives à la protection des informations classifiées.

44. L'article 19 alinéa 22 de la même loi dispose que le ministre de l'Intérieur soumet au Parlement des rapports annuels concernant les activités de la police nationale réglementées par l'article 19 §§ 1 à 21, lesquels rapports comportent les données et les informations visées à l'article 20 § 3 de ladite loi. Ils sont soumis au Parlement au plus tard le 30 juin de chaque année consécutive à celle sur laquelle ils portent.

2. La conservation des données de communication

45. Le régime juridique de la conservation des données de communication résulte d'une transposition en droit national de la directive 2006/24/EU sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE adoptée le 15 mars 2006 (la « directive sur la conservation des données », paragraphe 97 ci-dessous), laquelle transposition a été effectuée par la loi modificative de la loi sur les télécommunications et les autres lois du 24 avril 2009.

46. L'article 20 c de la loi sur la police réglemente ce type de surveillance. Selon cette disposition, la police peut conserver des données de communication aux fins de prévention ou détection des activités criminelles, de sauvetage de vies humaines ou de protection de la santé, ou encore de réalisation d'opérations de recherche et de sauvetage. L'accès aux données ne permet pas de connaître le contenu des communications privées. Le terme « données de communication» englobe les données liées aux télécommunications visées à l'article 180 c et d de la loi sur les télécommunications (paragraphe 61 ci-dessous), celles relatives aux communications postales au sens de l'article 82 alinéa 1 point 1 de la loi sur la poste (*Ustawa Prawo pocztowe*,

paragraphe 62 ci-dessous), ainsi que celles afférentes aux communications numériques visées à l'article 18 alinéas 1 à 5 de la loi sur la prestation de services en ligne (paragraphe 63 ci-dessous). Il inclut également les informations relatives, entre autres, aux appels téléphoniques effectués ou reçus, aux numéros composés, à la durée des appels, à la localisation géographique des appareils mobiles à tel ou tel moment, aux sites Internet consultés, aux connexions à des sites, aux paramètres personnels et aux adresses de correspondance e-mail. Les données ainsi collectées sont traitées à l'insu de la personne concernée et sans son consentement. Les prestataires de services de technologies de l'information et de la communication (les « services TIC ») sont tenus d'accorder aux agents de police compétents un accès gratuit aux données en question (l'article 20 c § 2 de la même loi). Chacun des autres services de l'État concernés peut procéder à la collecte de données de communication pour autant qu'elle est nécessaire à la réalisation des buts statutaires du service en cause.

47. L'article 20 c § 3 de la loi sur la police prévoit la possibilité pour la police de passer avec les prestataires de services TIC des conventions confidentielles lui assurant un accès direct aux données de communication, sans intervention du personnel du prestataire concerné. Les fonctionnaires de police compétents tiennent des registres électroniques confidentiels dans lesquels sont consignées les demandes d'accès aux données. Les moyens techniques par lesquels la police met en œuvre les mesures de conservation des données de communication sont eux aussi confidentiels.

48. Les données visées à l'article 20 c § 1 de ladite loi qui présentent une utilité au regard d'une procédure pénale en cours d'instruction sont transmises par les agents de police compétents au procureur compétent, lequel décide de l'utilisation qui en sera faite. Les données qui sont dépourvues de toute utilité pour une procédure pénale sont détruites sans délai par une commission protocolaire.[3]

49. L'article 20 ca de la même loi réglemente quant à lui le contrôle de l'obtention de données de communication par les services de la police. Cette disposition impose à la police de soumettre à la juridiction régionale compétente un rapport semestriel contenant des informations générales concernant, d'une part, le nombre de cas d'accès aux données répertoriées au cours de la période considérée, accompagné d'une indication du type de données en cause et, d'autre part, les qualifications juridiques auxquelles les demandes d'accès aux données en question se rapportaient, ainsi également que des informations relatives à l'obtention de données visant à la protection de vies humaines et de la santé ou au soutien de missions de recherche ou de sauvetage. Aux fins de l'exercice d'un contrôle plus approfondi sur certaines des affaires concernées, le tribunal compétent peut prendre connaissance du contenu des éléments qui ont justifié le recours à ladite mesure de la part de la police. Le tribunal informe la police des conclusions auxquelles il est parvenu à l'issue de son contrôle dans un délai de trente jours à compter de l'achèvement de celui-ci.

50. L'article 20 cb de la loi concerne le traitement des données relatives aux abonnements. En application de l'article 20 ca 5), l'acquisition et le traitement desdites données sont exclus du contrôle *a posteriori* prévu par cette disposition.

3. *La loi anti-terrorisme*

51. La loi anti-terrorisme réglemente les méthodes utilisées dans le cadre de la lutte contre le terrorisme et en matière de coopération entre les autorités compétentes dans ce domaine.

52. L'article 2 de cette loi définit les termes clés aux fins de l'application de la loi. Selon cette disposition, la notion d'« actions antiterroristes » (*działania antyterrorystyczne*) recouvre l'ensemble des mesures que les autorités peuvent mettre en œuvre pour prévenir les « incidents à caractère terroriste », se préparer à prendre le contrôle de tels incidents, réagir à leur survenance et faciliter l'élimination de leurs conséquences, y compris par l'utilisation des ressources destinées à y faire face. Les « actions contre-terroristes » (*działania kontrterrorystyczne*), au sens de cette même loi, sont quant à elles les actions qui sont menées contre les auteurs des infractions à caractère terroriste visées à l'article 115 § 2 du code pénal (*Kodeks karny* – « le CP ») et de leurs complices au moyen de ressources, de méthodes et de plans d'action spéciaux en cas de danger imminent pour la vie, la santé humaine, la liberté personnelle des individus et les biens. La notion d' « incidents à caractère terroriste » englobe quant à elle l'ensemble des situations susceptibles d'avoir été causées par la commission d'une infraction à caractère terroriste au sens de l'article 115 § 2 du CP ou révélant l'existence d'un risque de commission d'une telle infraction.

53. Des mesures de surveillance peuvent être mises en place à l'égard des ressortissants étrangers soupçonnés d'activités terroristes.

54. L'article 9 § 1 de ladite loi comporte la liste des mesures que les agents de l'ABW peuvent appliquer en secret, pendant une période n'excédant pas trois mois, à l'endroit des étrangers en question. Elle comprend notamment l'enregistrement du contenu de conversations téléphoniques et de correspondances entretenues *via* les réseaux de télécommunications et de communications numériques, les enregistrements sonores, la prise d'images de lieux et de moyens de transport privés, l'enregistrement de données inscrites sur des supports informatiques, des dispositifs de télécommunication ou des systèmes informatiques et téléinformatiques et le contrôle de colis postaux. La décision de recourir à ces mesures est motivée, et elle est prise par le chef de l'ABW. Celui-ci en informe sans délai le ministre chargé de la supervision des services spéciaux de l'État et le procureur en chef du parquet national. Ce dernier peut mettre fin aux mesures de surveillance engagées.

55. Selon l'article 9 § 5 de la même loi, les mesures de surveillance secrète mises en place peuvent être renouvelées dans les conditions prévues à l'article 27 de la loi sur l'ABW et les services de renseignement[4].

56. Le chef de l'ABW informe sans délai le procureur en chef du parquet national des conclusions qui ressortent des mesures de surveillance secrète et, en cas de demande faite en ce sens par ce dernier, de la manière dont lesdites mesures ont été appliquées, avant de lui transmettre les éléments recueillis dans le cadre de celles-ci. Le procureur en chef du parquet national décide de la portée et du mode d'utilisation de ces éléments. Les dispositions des articles 238 §§ 3-5 et 239 du CPP (paragraphe 58 ci-dessous) s'appliquent *mutatis mutandis*.

57. Le procureur en chef du parquet national ordonne la destruction des éléments issus des mesures de surveillance secrète dès lors que ceux-ci ne sont pas constitutifs d'un moyen de preuve concernant la commission d'une infraction et qu'ils ne sont d'aucune pertinence pour la sécurité de l'État.

4. Le code de procédure pénale

58. Les dispositions du CPP pertinentes en l'espèce sont ainsi libellées :

Article 178

« Ne peut être interrogé comme témoin : 1) un avocat de la défense ou un conseiller juridique agissant en vertu de l'article 245 § 1 [du présent code] ou un avocat relativement à des faits dont il a eu connaissance à l'occasion d'un conseil juridique ou de la conduite d'une affaire 2) un ecclésiastique relativement à des faits dont il a eu connaissance lors d'une confession. »

Article 178a

« Ne peut être interrogé comme témoin un médiateur au sujet de faits révélés par un accusé ou une victime lors de la conduite d'une procédure de médiation, à l'exception des informations sur les infractions visées à l'article 240 § 1 du code pénal. »

Article 179

« § 1. Les personnes tenues de ne pas divulguer des informations classées "confidentielles" ou "strictement confidentielles" ne peuvent témoigner au sujet des informations auxquelles s'applique l'obligation susmentionnée qu'après avoir été exonérées de l'obligation de confidentialité par une autorité supérieure compétente.

§ 2. Une exonération ne peut être refusée que dans le cas où le témoignage risquerait d'occasionner un préjudice grave à l'État.

§ 3. Le tribunal ou le ministère public peut demander à l'administration compétente de délier un témoin de son obligation de confidentialité, à moins que des lois spécifiques n'en disposent autrement. »

Article 180

« § 1. Les personnes tenues de ne pas divulguer des informations classées "privilégiées" ou "confidentielles" ou des secrets liés à leur profession ou à leurs fonctions peuvent refuser de témoigner concernant des informations couvertes par cette obligation, à moins que le tribunal ou le procureur général, agissant dans l'intérêt de l'administration de la justice, ne les libère du devoir de confidentialité et pour autant que des lois spécifiques n'en disposent autrement. Les décisions relatives à une exonération du devoir de confidentialité peuvent faire l'objet d'un appel interlocutoire.

§ 2. Les personnes bénéficiant du privilège du notaire, de l'avocat, du conseiller juridique, du conseiller fiscal, du médecin, du journaliste, du statisticien ou du conseiller général de la République de Pologne ne peuvent être interrogées sur les faits couverts par ce privilège que lorsque cela est indispensable dans l'intérêt de l'administration de la justice et que ces faits ne peuvent être établis sur la base d'aucune autre preuve. Dans les procédures préparatoires, le tribunal statue lors d'une audience sans la présence des parties et dans un délai n'excédant pas sept jours à compter de la demande du procureur général tendant à une déposition [devant le tribunal] ou à une autorisation de prise de déposition. La décision du tribunal peut faire l'objet d'un appel interlocutoire.

§ 3. L'exonération de l'obligation au secret des journalistes ne peut s'appliquer aux informations permettant d'identifier l'auteur d'un document de presse, d'une lettre à l'éditeur

ou de tout autre document de cette nature, ou des personnes fournissant des informations publiées ou destinées à être publiées qui ont demandé que lesdites informations soient couvertes par le privilège.

§ 4. Les dispositions du paragraphe 3 ne s'appliquent pas si l'information concerne l'infraction visée à l'article 240 § 1 du code pénal.

§ 5. Le refus du journaliste de divulguer des informations visées au paragraphe 3 ne l'exonère pas de la responsabilité encourue pour un délit qu'il commet en publiant l'information. »

Article 238

« § 1. La surveillance et la mise sur écoute téléphonique peuvent être imposées pour une période maximale de trois mois, qui peut être prolongée dans des cas jugés particulièrement justifiés pour une période supplémentaire n'excédant pas trois mois.

§ 2. La surveillance doit prendre fin immédiatement après que les circonstances mentionnées à l'article 237 § 1-3 ont cessé d'exister, et au plus tard à l'expiration de la durée pour laquelle elle a été imposée.

§ 3. À l'issue de la surveillance, si les enregistrements sont sans importance pour la procédure pénale dans son ensemble, le procureur général dépose une requête pour qu'ils soient tous détruits. Le tribunal statue immédiatement sur celle-ci, lors d'une audience qui se tient sans la participation des parties.

§ 4. Après la clôture de la procédure préparatoire, le procureur national dépose une requête en vue de la destruction des passages des enregistrements qui sont sans rapport avec la procédure pénale pour laquelle la surveillance et la mise sur écoute téléphonique ont été ordonnées et qui ne sont pas constitutifs d'une preuve visée à l'article 237a. Le tribunal statue sur la requête lors d'une audience à laquelle les parties peuvent assister.

§ 5. Une requête visant à obtenir une ordonnance de destruction des enregistrements peut également être présentée par la personne visée à l'article 237 § 4, au plus tôt après la conclusion de la procédure préparatoire. Le tribunal statue sur la requête lors d'une audience à laquelle les parties et le requérant peuvent assister. »

Article 239

« §1. La notification de l'ordonnance autorisant la surveillance et la mise sur écoute téléphonique à la personne concernée peut être reportée pendant la durée nécessaire à la protection des intérêts de l'affaire.

§ 2. Dans une enquête préliminaire, la notification de l'ordonnance visée au paragraphe 1 ne peut être reportée au-delà de la conclusion de la procédure. »

Article 321

« § 1. Lorsqu'il existe des motifs de clôture de l'enquête, sur demande du suspect ou de son défenseur tendant à la consultation des pièces de la procédure, l'autorité chargée de l'enquête informe l'un ou l'autre de la date à laquelle ils pourront consulter lesdites pièces. Il leur est également indiqué qu'avant de prendre connaissance de celles-ci, ils peuvent examiner le

dossier dans un délai que l'autorité chargée de la procédure fixe en fonction de l'importance et de la complexité de l'affaire. Aux fins de leur examen, les dossiers peuvent être rendus disponibles sous forme électronique.

§ 2. La date à laquelle le suspect peut prendre connaissance des documents de la procédure doit être fixée [de manière à ce qu'il dispose] d'un délai d'au moins sept jours à compter de la notification de ladite date à lui ou à son défenseur.

§ 3. L'avocat de la défense a le droit de participer aux actes visant à permettre au suspect de prendre connaissance des éléments de la procédure avant la clôture de l'enquête.

§ 4. Le défaut de comparution injustifié du suspect ou de son défenseur ne met pas fin à la procédure.

§ 5. Dans les trois jours suivant l'examen des pièces de l'enquête, les parties peuvent présenter des demandes de complément d'enquête. L'article 315 § 2 s'applique en conséquence.

§ 6. S'il n'y a pas lieu de poursuivre l'enquête, la décision de clôture est rendue et annoncée, ou son contenu est communiqué, au suspect et à son défenseur. »

Article 393

« § 1. Peuvent être lus au procès les transcriptions des inspections, perquisitions et saisies d'objets, les avis d'experts, d'instituts, d'établissements et d'institutions, les casiers judiciaires, les conclusions d'enquête de voisinage, ainsi que tous les documents officiels présentés au cours des procédures préparatoires, des procédures judiciaires ou de toute autre procédure prévue par la loi. Toutefois, la lecture des notes relatives aux actes [de procédure] qui doivent faire l'objet une transcription dans un procès-verbal est prohibée.

(...) »

5. La loi du 6 septembre 2001 sur l'accès à l'information publique

59. Les dispositions pertinentes en l'espèce de la loi sur l'accès à l'information publique se lisent comme suit :

Article 1

« 1. Toute information relative aux affaires publiques constitue une information publique au sens de la présente loi et doit être rendue publique dans les conditions et selon les modalités précisées par celle-ci.

2. Les dispositions de la [présente] loi sont sans préjudice des dispositions des lois portant réglementation de l'accès aux informations publiques des citoyens. »

Article 2

« 1. Toute personne a le droit d'accéder aux informations publiques, sous réserve des dispositions de l'article 5.

2. Il ne peut être exigé de celui qui exerce son droit d'accès à l'information publique qu'il démontre avoir un intérêt en ce sens.

(...) »

Article 5

« Le droit à l'information publique fait l'objet des restrictions prévues par les dispositions relatives à la protection des informations classifiées et aux secrets protégés par la loi, selon les modalités qui y sont énoncées.

(...) »

Article 10

« Les informations publiques qui n'ont fait l'objet d'une publication ni au bulletin d'information publique ni sur le site [Internet] dédié sont communiquées [à celui qui en fait] la demande.

(...) »

Article 16

« 1. Dans la situation indiquée à l'article 14 alinéa 2, le rejet par l'autorité publique compétente d'une demande de communication d'informations publiques [formée par un individu] et l'abandon de la procédure y relative font l'objet d'une décision [écrite].

2. Les dispositions du CPA s'appliquent aux décisions indiquées à l'alinéa 1, à l'exception de ce qui suit :

1) le délai d'examen des recours contre les décisions en question est de quatorze jours ;

2) les décisions susvisées précisent les noms, prénoms et fonctions des auteurs de la décision ainsi que les dénominations des entités dont les intérêts légitimes (...) ont été pris en compte à l'appui de celle-ci. »

6. La loi du 5 août 2010 sur la protection des données classées

60. Les dispositions pertinentes en l'espèce de la loi sur la protection des données classées énoncent ce qui suit :

Article 4

« 1. Les informations classifiées sont communiquées uniquement à celui qui présente des garanties quant au respect du secret en la matière et seulement pour autant que nécessaire à l'accomplissement des missions qui lui sont dévolues.

2. Les dérogations à la règle de confidentialité des informations classifiées et les principes régissant l'utilisation dans des procédures diligentées par les tribunaux et les autres autorités publiques des dossiers contenant ces informations font l'objet d'une réglementation législative distincte.

3. Si, en application des dispositions spécifiques [prévues par la présente loi], des autorités, services ou organismes publics ou des membres de leur personnel respectif se voient accorder une autorisation de procéder à des contrôles portant sur des informations classifiées et, plus particulièrement, une autorisation d'accéder librement aux locaux et [aux différents] éléments

[pertinents à cette fin], les attributions [dévolues auxdits organismes respectifs] s'exercent [dans le respect] des dispositions de la présente loi. »

Article 5

« 1. Sont classées « strictement secrètes » les informations dont la communication en l'absence de l'autorisation requise serait susceptible de porter une atteinte particulièrement grave [aux intérêts de] la République de Pologne et pourrait, en particulier :

1) menacer son indépendance, sa souveraineté ou son intégrité territoriale ;

2) menacer sa sécurité intérieure ou son ordre constitutionnel ;

3) remettre en question ses alliances ou son rang au sein de la communauté internationale ;

4) affaiblir sa capacité de défense ;

5) conduire ou être susceptible de conduire à la divulgation de l'identité d'agents (...) des services de renseignement ou de contre-espionnage (...) et nuire à la bonne marche des opérations menées par eux ou conduire à l'identification des personnes qui les assistent dans la mise en œuvre de ces opérations ;

6) représenter un danger pour la vie ou la santé des [agents] qui effectuent des missions opérationnelles et de reconnaissance ou de ceux qui les assistent lors de ces opérations ;

7) représenter un danger pour la vie ou la santé de repentis ou de leurs proches, de personnes qui ont bénéficié des mesures de protection et d'assistance prévues par la loi du 28 novembre 2014 relative à la protection et à l'assistance des victimes et des témoins (Journal des lois de 2015, considérant 21) ou de témoins visés à l'article 184 du CPP ou de leurs proches.

2. Sont classées « secrètes » les informations dont la communication en l'absence de l'autorisation requise à cette fin serait susceptible de porter une atteinte particulièrement grave [aux intérêts de] la République de Pologne et pourrait, en particulier :

1) nuire à la bonne marche de missions de sauvegarde de sa souveraineté ou de son ordre constitutionnel ;

2) entraîner une détérioration de ses relations avec les autres États ou les organisations internationales ;

3) perturber des opérations menées en vue de sa défense ou nuire à la bonne marche des opérations de ses forces armées ;

4) entraver la bonne marche d'activités opérationnelles et de reconnaissance visant à la préservation de sa sécurité ou à la poursuite des auteurs d'infractions (...) ;

5) occasionner de graves perturbations pour les forces de l'ordre et le système judiciaire ;

6) causer un préjudice grave à ses intérêts économiques.

3. Sont classées « confidentielles » les informations dont la communication en l'absence de l'autorisation requise à cette fin serait susceptible de porter atteinte [aux intérêts de] la République de Pologne et pourrait, en particulier :

1) entraver la conduite de sa politique étrangère ;

2) nuire à ses missions et à ses capacités de défense nationale ;

3) occasionner un trouble à l'ordre public ou à la sécurité des citoyens ;

4) nuire à l'accomplissement de missions qui sont dévolues aux organismes de protection de la sécurité nationale ou de ses intérêts fondamentaux ;

5) nuire à l'accomplissement de missions qui sont dévolues aux autorités judiciaires et aux organismes de protection de l'ordre public et de la sécurité, de la répression des auteurs des infractions à la loi fiscale ;

6) perturber la stabilité de son système budgétaire ;

7) nuire au bon fonctionnement de l'économie nationale.

4. Sont classée « restreintes » les informations qui ne relèvent pas des niveaux de protection [visés aux paragraphes 1-3] mais dont la divulgation pourrait nuire à l'accomplissement par les organismes habilités de missions qui leur sont dévolues en matière de défense nationale, de politique étrangère, de sécurité publique, de préservation des droits et libertés des citoyens, d'administration de la justice ou de sauvegarde des intérêts économiques de l'État.

5. Les informations classifiées dont la transmission [aux autorités polonaises] par leurs homologues des autres États ou par les organisations internationales s'effectue en application d'accords internationaux obtiennent le niveau de protection équivalent à celui dont elles faisaient l'objet [avant leur transmission]. »

7. La loi du 16 juillet 2004 sur les télécommunications

61. Les dispositions pertinentes en l'espèce de la loi sur les télécommunications disposent ce qui suit :

Article 159

« 1. Le secret des correspondances émises par voie de télécommunications concerne :

1) les données de l'utilisateur ;

(...)

3) les données de transmission, à savoir, les données traitées en vue de la transmission de contenus par les réseaux de télécommunications ou de la facturation de services de télécommunications, y compris les données de localisation, c'est-à-dire l'ensemble des données traitées par les réseaux de télécommunications ou dans le cadre de services de télécommunications indiquant la localisation géographique de l'équipement terminal d'un utilisateur de services de télécommunications accessibles au public ;

4) les données de localisation autres que celles qui sont nécessaires à la transmission d'un message ou à la facturation ;

5) les données relatives aux tentatives de connexion, y compris celles relatives aux connexions qui n'ont pas été établies, entre l'équipement terminal de télécommunications et le point terminal du réseau, à savoir celles qui n'ont pas été reçues par l'utilisateur final ou qui ont été interrompues.

(...) »

Article 161

« 1. Sous réserve des dispositions du paragraphe 2, les contenus ou les données couverts par le secret des correspondances émises par voie de télécommunications ne peuvent être collectés, enregistrés, stockés, traités, modifiés, effacés ou communiqués que si ces activités,

ci-après dénommées « traitement », concernent le service fourni à l'utilisateur ou sont nécessaires à sa fourniture. Leur traitement à d'autres fins ne peut intervenir qu'en application des dispositions [distinctes de celles de la présente loi].

(2) Le fournisseur de services de télécommunications accessibles au public peut traiter les données énoncées ci-dessous lorsque l'utilisateur est une personne physique :

1) les noms et prénoms ;

2) les prénoms des parents ;

3) le lieu et la date de naissance ;

4) l'adresse de domiciliation et l'adresse de correspondance si elle est différente de la première ;

5) le numéro d'identification PESEL – dès lors qu'il s'agit d'un ressortissant polonais ;

6) le nom, la série et le numéro des pièces d'identité et, dans le cas d'un ressortissant étranger qui n'est pas ressortissant d'un État membre [de l'Union européenne] ou de la Confédération suisse, le numéro du passeport ou de la carte de séjour ;

7) les informations figurant sur les documents attestant de la capacité [de l'utilisateur] de s'acquitter des créances vis-à-vis du fournisseur de services de télécommunications accessibles au public découlant du contrat de fourniture de [tels] services.

(3) Hormis les données indiquées au paragraphe 2, le fournisseur de services de télécommunications accessibles au public peut, avec l'accord de l'utilisateur qui est une personne physique, traiter les autres données relatives à l'utilisateur qui se rapportent au service fourni, dont le numéro de compte bancaire ou de carte de crédit, l'adresse électronique et les coordonnées téléphoniques. »

Article 179

« (...)

(9) Le fournisseur de services de télécommunications accessibles au public est tenu d'établir un registre sous forme numérique des abonnés, des utilisateurs ou des équipements terminaux de télécommunications, et d'y inclure les données collectées par lui à l'occasion de la conclusion des contrats [auxquels il est partie]. »

Article 180a

« 1. Sous réserve des dispositions de l'article 180c paragraphe 2 alinéa 2, l'opérateur de réseau public de télécommunications et le fournisseur de services de télécommunications accessibles au public sont tenus d'accomplir, à leurs frais, [les opérations suivantes] :

1) retenir et conserver, pendant une période d'une durée de douze mois à compter de la date de connexion [...], les données qui sont précisées à l'article 180c et qui sont générées par le réseau de télécommunications ou traitées par eux sur le territoire de la République de Pologne et, à l'expiration dudit délai, procéder à la destruction [des données en question] excepté celles qui ont fait l'objet d'un archivage en application de dispositions distinctes [de celles de la présente loi] ;

2) mettre les données [en question] à disposition des organismes habilités et, tout particulièrement, du tribunal et du procureur [compétents] selon les règles et modalités [pertinentes] prévues par des dispositions distinctes [de celles de la présente loi] ;

3) protéger les données mentionnées au paragraphe 1 d'une destruction accidentelle ou involontaire, d'une suppression ou d'une modification [injustifiées], d'une conservation irrégulière ou illégitime, d'un traitement, d'une interception ou d'une divulgation (...).

2. Sous réserve des dispositions du paragraphe 3, l'obligation énoncée au paragraphe 1 est considérée comme remplie [par l'opérateur du réseau de télécommunications ou le fournisseur de services de télécommunications accessibles au public] en cas de transmission [à leurs éventuels homologues], consécutivement à leur cessation d'activité, [des données en question] en vue de leur conservation, divulgation ou protection subséquentes.

3. En cas de faillite, l'opérateur du réseau de télécommunications ou le fournisseur de services de télécommunications accessibles au public doivent transmettre les données indiquées au paragraphe 1 au responsable en chef du Bureau des communications électroniques (« UKE »).

(...)

5. Sont concernées par l'obligation énoncée au paragraphe 1 les données relatives aux connexions réalisées et aux connexions, précisées à l'article 159 paragraphe 1 alinéa 5, qui n'ont pas été établies.

6. L'obligation énoncée au paragraphe 1 est mise en œuvre de façon à ce que les télécommunications transmises ne soient pas divulguées.

7. Une mise à disposition des données précisées au paragraphe 1 s'effectue *via* le réseau de télécommunications, sauf disposition contraire. »

Article 180c

« 1. Sont visées par l'obligation énoncée ci-dessus à l'article 180a alinéa 1 les données qui sont nécessaires :

1) à l'identification d'une interface réseau, d'un équipement terminal de télécommunications ou de l'utilisateur final :

a) établissant la communication,

b) vers lequel la communication est émise ;

2) à l'identification :

a) de la date, de l'heure et de la durée de la communication,

b) du type de communication [en cause],

c) de la localisation de l'équipement terminal de télécommunications.

2. Le ministre de la Transition numérique, statuant en concertation avec le ministre de l'Intérieur, (...) détermine par voie réglementaire :

1) une liste détaillée des données mentionnées à l'alinéa 1 ;

2) les catégories d'exploitants de réseaux publics de télécommunications ou de fournisseurs de services de télécommunications accessibles au public qui sont tenus par l'obligation de conservation et d'archivage de ces données. »

Article 180d

« Les opérateurs de télécommunications sont tenus d'assurer, à leurs frais, [d'une part], les conditions propres à rendre les données indiquées aux articles 159 § 1 alinéas 1, 3-5, 161 et 179 § 9 [de la présente loi] qui sont traitées par eux relativement au service de télécommunications qu'ils fournissent accessibles aux organismes habilités, aux tribunaux et au parquet et, [d'autre part], l'enregistrement et la mise à disposition [auprès de ceux-ci des données en question] dans les conditions et selon les modalités précisées par des dispositions législatives distinctes [de la présente loi], ainsi que dans le respect des procédures prévues par celles-ci. »

8. La loi du 23 novembre 2012 sur la poste

62. Les dispositions pertinentes en l'espèce de la loi sur la poste sont ainsi libellées :

Article 82

« 1. L'opérateur postal (...) est tenu d'assurer à ses frais (...) les conditions techniques et organisationnelles qui sont nécessaires à l'accomplissement par la police, la police des frontières, l'ABW, le SKW, la ŻW, le CBA, le KAS, les services de protection de l'État (« les SOP ») (...), le ministère public et les tribunaux des missions qui leur sont dévolues en application de lois distinctes [de la présente loi] et dont la réalisation requiert :

1) une communication des informations relatives à l'opérateur postal [concerné] et aux services postaux fournis par lui ainsi que celles qui rendent possible l'identification des utilisateurs de ces services,

2) une mise à disposition de colis propre à permettre le contrôle de leur contenu,

3) une mise à disposition en vue de leur examen par les services de l'État compétents de colis retenus par l'opérateur qui sont susceptibles de contenir des objets issus d'une activité criminelle,

4) une autorisation d'acheminement concernant un colis pouvant contenir des objets issus d'une activité criminelle (...) – selon les modalités qui sont précisées dans des dispositions législatives spécifiques. »

9. La loi du 18 juillet 2002 sur la prestation de services en ligne

63. La loi sur la prestation de services en ligne énonce ce qui suit :

Article 18

« 1. Le prestataire [de services par voie électronique] peut traiter, dans la limite de ce qui est nécessaire à l'établissement d'un contrat, à la détermination du contenu de celui-ci ainsi qu'à sa modification ou à sa résiliation, les données personnelles du destinataire [des services en question] exposées ci-après :

1) nom et prénoms du destinataire ;

2) numéro [national d'identité] PESEL ou à défaut numéro de passeport, de carte d'identité ou d'un autre document d'identité ;

3) adresse de domiciliation ;

4) adresse de correspondance si elle diffère de celle indiquée à l'alinéa3 ;

5) informations nécessaires à la vérification de la signature électronique du destinataire ;

6) adresses électroniques de celui-ci.

2. Aux fins de l'exécution du contrat ou de l'accomplissement d'actes juridiques impliquant le destinataire, le prestataire de services [susmentionné] peut traiter d'autres données personnelles de celui-ci en cas de nécessité résultant de la nature du service fourni ou de son mode de règlement.

3. Le prestataire de services identifie les données précisées au paragraphe 2 dont la communication est nécessaire à la fourniture du service par voie électronique, conformément à l'article 22 § 1, et il établit le relevé des données en question.

4. Le prestataire de services peut traiter, avec le consentement du destinataire et à des fins de publicité, d'étude de marché et de recherche sur le comportement et les préférences des destinataires du service ou dans le but d'améliorer la qualité des services fournis par le prestataire de services, d'autres données du destinataire qui ne sont pas indispensables à la fourniture du service par voie électronique.

5. Le prestataire de services peut traiter les données ci-après relatives au service fourni par voie électronique (données opérationnelles) :

1) identifiant le destinataire sur la base des données précisées au paragraphe 1 ;

2) identifiant le système informatique utilisé par le destinataire ou la terminaison du réseau de télécommunications ;

3) contenant des informations sur le début, la fin et la portée de chaque utilisation d'un service électronique ;

4) contenant des informations sur l'utilisation par le destinataire des services fournis par voie électronique.

6. Le prestataire de services met gratuitement à disposition des autorités publiques habilitées par des dispositions distinctes [de la présente loi] les données précisées aux alinéas 1-5 qui sont utiles aux procédures diligentées par les autorités publiques en question. »

10. La loi sur le Parquet (Ustawa o Prokuraturze) *du 28 janvier 2016*

64. Les articles pertinents en l'espèce de la loi sur le Parquet se lisent ainsi :

Article 1

« (...)

§ 2. Le procureur en chef du parquet national est l'organe suprême du parquet. Cette fonction est exercée par le ministre de la Justice. (...) »

Article 11

« § 1. Le procureur en chef du parquet national présente au Parlement une note d'information annuelle relative au nombre d'individus pour lesquels une demande de mise en place d'un contrôle opérationnel a été formulée, qui précise le nombre de ceux des individus concernés :

1) pour lesquels un tribunal a ordonné un contrôle opérationnel,

2) pour lesquels un tribunal a rejeté une demande de mise en place du contrôle opérationnel,

3) pour lesquels un procureur n'a pas consenti à la mise en place du contrôle opérationnel,

(...)

§ 2. La note d'information susmentionnée est présentée au Parlement au plus tard le 30 juin de l'année suivant celle à laquelle elle se rapporte. »

Article 13

« § 1. Le procureur en chef du parquet national dirige le parquet (...).

§ 2. Les procureurs (...) sont subordonnés au procureur en chef du parquet national. »

11. La loi sur le CBA

65. L'article 12 §§ 3 et 4 de cette loi prévoit, d'une part, que le chef du CBA présente chaque année, au plus tard le 31 mars, au Premier ministre et à la commission parlementaire supervisant les services secrets un rapport d'information concernant les opérations qui ont été diligentées au cours de l'année antérieure par les services qu'il dirige et, d'autre part, qu'il communique au Parlement les résultats des opérations qui ne relèvent pas du champ d'application des dispositions relatives à la protection des données classifiées.

12. *La loi du 27 juillet 2001 sur l'organisation des tribunaux ordinaires* (Ustawa Prawo o ustroju sądów powszechnych)

66. L'article 175b §§ 1 et 2 de cette loi énonce que les présidents des tribunaux régionaux territorialement compétents communiquent chaque année au ministre de l'Intérieur des éléments d'information sur le traitement des données liées aux télécommunications, aux communications postales et aux communications en ligne avec des précisions concernant le nombre de demandes d'accès aux données en question qui ont été favorablement accueillies et les conclusions des contrôles ordonnés par eux dans ce domaine. Il dispose en outre que le ministre de la Justice transmet annuellement au Parlement un recueil d'informations sur le traitement des données susvisées ainsi que les conclusions des contrôles qu'il a diligentés dans ce domaine.

13. Le code de procédure administrative

67. Les dispositions pertinentes en l'espèce du CPA sont ainsi libellées :

Article 227

« La plainte peut notamment porter sur une négligence ou un défaut d'exécution adéquate par les autorités publiques compétentes ou par leurs employés de leurs attributions respectives, sur la violation du principe de l'État de droit ou celle des intérêts des plaignants et sur la longueur excessive ou le traitement bureaucratique des dossiers. »

Article 228

« Les plaintes sont soumises aux autorités compétentes pour en connaître. »

Article 238

« § 1. La lettre informant des suites données à la plainte précise l'autorité publique [dont elle émane], la façon dont la plainte a été traitée et les coordonnées de la personne qui [avait] compétence pour la traiter (...). En cas de rejet de cette plainte, la lettre en précise les motifs juridiques et factuels et comporte les instructions relatives aux dispositions de l'article 239.

§ 2. Si la lettre susmentionnée est communiquée [à l'intéressé] par les services compétents de la Défense nationale, de l'Agence de sécurité intérieure, de l'Agence de renseignement extérieur, du Service de contre-espionnage militaire, du Service de renseignement militaire ou du Bureau central de lutte contre la corruption, les coordonnées de la personne compétente pour traiter les plaintes peuvent être omises. »

14. Le code civil (Kodeks cywilny – « le CC »)

68. En vertu de l'article 417[1] §§ 1, 2 et 4 du CC, quiconque estime avoir subi un préjudice du fait de l'adoption d'un acte normatif peut introduire une demande de réparation dès lors qu'il a été conclu, à l'issue d'une procédure pertinente, à l'incompatibilité dudit acte normatif avec la Constitution, un accord international ou une loi. Quiconque estime avoir subi un préjudice à raison d'une décision de justice ou d'une décision émanant d'une autorité publique peut, sauf disposition légale contraire, introduire une demande de réparation dès lors qu'à l'issue d'une procédure pertinente il a été conclu au caractère irrégulier de la décision en question, ou il a été établi que l'acte normatif sur lequel elle était fondée était contraire à la Constitution, à un accord international ou à une loi. Si un préjudice a été causé par la non-adoption d'un acte normatif dont l'édiction était obligatoire en vertu de la loi, le tribunal statuant sur une action indemnitaire introduite par la victime doit déterminer si la situation découlant de ladite omission législative était régulière ou non.

*15. La loi sur l'organisation de la Cour constitutionnelle et la procédure applicable à celle-ci (*Ustawa o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym - *« la loi sur la Cour constitutionnelle »)*

69. En vertu de l'article 77 § 1 de cette loi, un recours constitutionnel peut être déposé après l'épuisement des voies de recours, à supposer qu'elles existent, dans un délai de trois mois à compter de la date du prononcé de l'arrêt, de la décision ou de tout autre acte rendu à titre définitif.

16. La jurisprudence de la Cour constitutionnelle

a) L'arrêt K 32/04 du 12 décembre 2005

70. Dans l'affaire jugée par l'arrêt K 32/04 du 12 décembre 2005, le Commissaire aux droits de l'homme polonais avait saisi la Cour constitutionnelle d'une requête dans laquelle il soutenait, entre autres, que l'article 19 § 16 de la loi sur la police était incompatible avec plusieurs dispositions de la Constitution pour autant qu'il n'instaurait aucune obligation pour les fonctionnaires de police ayant procédé à un contrôle opérationnel de notifier celui-ci après son accomplissement, lorsque pareille notification pouvait se faire sans compromettre le but du

contrôle en question, à la personne qui y avait été soumise (excepté aux seuls accusé et à son défenseur).

71. Dans son arrêt, la Cour constitutionnelle a jugé que la disposition litigieuse s'opposait à ce qu'un contrôle opérationnel fût notifié pendant sa réalisation à la personne visée par celui-ci, mais qu'elle ne faisait pas obstacle à une notification après l'accomplissement de la mesure de surveillance en question lorsque celle-ci n'avait pas permis l'engagement de poursuites pénales contre l'individu concerné. La haute juridiction constitutionnelle a considéré que les personnes qui étaient soumises à un contrôle opérationnel devaient pouvoir, après la réalisation de celui-ci, exercer le droit, garanti par l'article 51 § 3 de la Constitution, de prendre connaissance des éléments collectés à leur insu dans le cadre de la surveillance en question. Elle a observé qu'en même temps, il convenait de distinguer entre, d'un côté, la situation en cause, où la législation applicable ne faisait aucunement obstacle à la notification du contrôle opérationnel à la personne qui en avait fait objet si celle-ci en faisait la demande, et, d'un autre côté, celle où les services de l'État qui avaient diligenté le contrôle opérationnel étaient tenus par une obligation de notification dudit contrôle, après sa cessation, à la personne visée. Elle a considéré que l'instauration de pareille obligation pour les services de l'État concernés serait souhaitable et utile à la mise en œuvre procédurale effective du droit énoncé à l'article 51 § 4 de la Constitution. Elle a indiqué en outre que d'autres États européens avaient rencontré un problème analogue, qui avait conduit à la hausse de leurs niveaux respectifs de protection procédurale des individus (citant l'exemple du législateur allemand, lequel, intervenant à la suite de l'affaire *Klass et autres (Klass et autres c. Allemagne*, arrêt du 6 septembre 1978, série A no 28) avait instauré l'obligation pour les autorités publiques compétentes d'informer, après la réalisation d'un contrôle opérationnel, la personne concernée de la mesure de surveillance diligentée à son insu). Elle a jugé qu'en l'espèce, le grief formulé par le Commissaire relativement à l'absence de notification du contrôle opérationnel à la personne visée découlait d'une lacune législative à laquelle elle-même ne pouvait remédier dans le cadre de son contrôle de la constitutionnalité des lois.

b) La décision S 2/06 du 25 janvier 2006

72. Par la décision S 2/06 du 25 janvier 2006, laquelle avait été consécutive à l'adoption de l'arrêt K 32/04 précité, la Cour constitutionnelle, donnant d'office des indications au législateur, a estimé qu'il était nécessaire d'adopter des mesures de protection supplémentaires à l'égard des personnes soumises à une surveillance en application de la loi sur la police et de procéder à un amendement analogue des lois dont les stipulations étaient similaires à celles qui avaient fait l'objet de son contrôle dans le cadre de l'arrêt susmentionné.

c) L'arrêt K 23/11 du 30 juillet 2014

73. L'affaire ayant donné lieu à l'arrêt K 23/11 du 30 juillet 2014 portait sur la constitutionnalité de plusieurs dispositions règlementant la mise en œuvre de contrôles opérationnels par divers services de police et de renseignement. La Cour constitutionnelle, statuant sur les demandes formées, respectivement, par le Commissaire aux droits de l'homme polonais et par le procureur en chef du parquet national, a déclaré certaines des dispositions mises en cause devant elle contraires à la Constitution. Dans les motifs de son arrêt, elle a observé ce qui suit :

– certaines des dispositions prévoyant les catalogues d'infractions pour lesquelles un contrôle opérationnel pouvait être mené étaient entachées d'imprécision. Tel était tout particulièrement le cas des dispositions pertinentes de la loi sur l'ABW et les services de renseignement, qui énonçaient le droit pour les services de l'ABW de diligenter un contrôle opérationnel relativement aux infractions « *contre les fondements économiques de l'État* ». En revanche, les dispositions applicables aux services de police, de contrôle fiscal, de police militaire et de police des frontières en vertu desquelles les services de l'État concernés étaient autorisés à diligenter des mesures de contrôle opérationnel relativement aux infractions « *réprimées en application des traités et des accords internationaux* » étaient conformes à la Constitution, sous réserve qu'elles fussent interprétées comme désignant les seules infractions réprimées en application du code pénal polonais et des accords internationaux ratifiés par le Parlement (ayant rang de loi). Il en allait de même des dispositions pertinentes de la loi sur l'ABW et les services de renseignement selon lesquelles les services compétents de l'ABW pouvaient recourir à un contrôle opérationnel relativement à d'« *autres* » infractions « *contre la sécurité de l'État* » ;

– il convenait de rejeter l'argument du Commissaire relatif à une imprécision des dispositions prévoyant les mesures techniques que les services de l'État pouvaient appliquer dans le cadre d'un contrôle opérationnel. La liste desdites mesures, bien qu'elle fût ample, n'était pas illimitée pour autant. Une règlementation trop succincte en la matière aurait nui aux impératifs de sécurité publique et à la bonne marche des opérations diligentées par les services de l'État concernés. Ce qui importait le plus dans ce contexte, c'était le fait que la législation applicable offrît aux individus visés de solides garanties de protection contre d'éventuels abus de la part desdits services de l'État. Or, parmi les garanties prévues par les dispositions litigieuses figurait l'obligation pour ceux-ci de préciser, dans leurs demandes d'autorisation de mise en place d'un contrôle opérationnel, les mesures techniques au moyen desquelles la surveillance en question serait effectuée. Par ailleurs, ces éléments devaient également être indiqués dans les décisions judiciaires autorisant la surveillance. De plus, la procédure d'autorisation des contrôles opérationnels, qui se déroulait en plusieurs étapes, constituait à elle seule une garantie importante de protection contre l'arbitraire concernant les mesures de surveillance mises en place. Il ressortait des éléments d'information dont elle disposait que le contrôle juridictionnel existant relativement à la légalité de la surveillance et à l'opportunité des mesures au moyen desquelles cette surveillance était réalisée était effectif ;

– les dispositions relatives à la transmission par les opérateurs du réseau public de télécommunications et par les fournisseurs de services de télécommunications des données de communication aux services de police et de renseignement étaient contraires à la Constitution pour autant qu'elles ne prévoyaient aucun mécanisme propre à assurer un contrôle indépendant des services de l'État desdites transmissions. Il en allait de même des dispositions pertinentes de la loi sur l'ABW et les services de renseignement, de la loi sur le CBA et de la loi sur le SKW pour autant qu'elles excluaient *expressis verbis* tout contrôle externe indépendant en la matière. Il découlait des termes des dispositions précisant les infractions pour lesquelles la mesure de surveillance en question pouvait être mise en place que celle-ci pouvait concerner n'importe quelle infraction, y compris la plus banale. De plus, les autorités recourant à pareille mesure n'étaient pas tenues de démontrer que celle-ci fût respectueuse du principe de

subsidiarité et nécessaire dans les circonstances en cause. Le fait que seuls les agents des services de l'État concernés étant pourvus des attestations de sécurité requises puissent engager une surveillance de ce type ne fournissait pas à la personne visée une garantie suffisamment solide contre d'éventuels abus de leurs part. Les particularités de la surveillance en question l'amenaient (la Cour constitutionnelle) à conclure que le mécanisme de contrôle le plus adéquat en la matière était celui du contrôle *a posteriori*. Ainsi, l'instauration d'une obligation d'autorisation à l'égard de toute mesure de surveillance, quel que fût son degré d'intrusion dans la sphère privée de la personne visée, ne s'imposait pas. Cependant, le législateur devait envisager d'introduire un contrôle *a priori* à l'égard des mesures diligentées dans des situations non urgentes ou en cas de collecte par les services de l'État procédant à la surveillance d'éléments couverts par le secret professionnel. Le contrôle des mesures de surveillance ne devait pas nécessairement être un contrôle juridictionnel, mais il devait être conforme des principes dégagés en la matière par la Cour européenne des droits de l'homme et la CJUE et, en particulier, être confié à un organisme indépendant du pouvoir exécutif ;

– la législation contestée[5], pour autant qu'elle ne prévoyait aucune procédure de destruction des éléments relevant du privilège de l'avocat ou du journaliste, ou du secret de la confession, qui avaient été collectés dans le cadre d'un contrôle opérationnel sans que le privilège en question n'eût été levé par un tribunal ou alors qu'une loi faisait obstacle à pareille levée, était contraire à la Constitution. S'il n'était, certes, pas opportun d'exclure de manière absolue les communications entre les avocats et leurs clients du champ d'application de la surveillance, les enjeux que lesdites communications comportaient pour les droits de la défense étaient tels que leur confidentialité devait faire l'objet d'une protection accrue non seulement à tous les stades de la procédure pénale, mais aussi dans le cadre des surveillances menées en dehors ou en amont de pareille procédure. Dès lors que la surveillance des communications des dépositaires du secret professionnel n'était pas prohibée en soi, il était impératif qu'elle fût assortie de garanties adéquates visant à protéger les personnes visées contre toute surveillance abusive et à empêcher les services de l'État concernés de se procurer indûment des informations couvertes par le secret professionnel. Le mécanisme d'exonération du secret professionnel édicté à l'article 180 § 2 du CPP pouvait constituer le modèle de référence en la matière, et la législation réglementant le recours à la surveillance en amont d'une procédure pénale devait instaurer un système analogue, celui-ci devant être à même, d'une part, de permettre aux services de l'État effectuant la surveillance d'identifier, préalablement à une transmission aux autres organismes, celles des informations collectées par eux qui étaient couvertes par le secret professionnel et, d'autre part, de conduire à la destruction par une commission protocolaire de l'ensemble des éléments en question ;

– les dispositions pertinentes de la loi sur l'ABW et les services de renseignement, de la loi sur le SKW et le service de renseignement militaire et de la loi sur la CBA étaient également contraires à la Constitution pour autant qu'elles n'édictaient aucune réglementation en matière de destruction des données de communication qui s'étaient révélées inutiles aux procédures pour lesquelles elles avaient été collectées.

d) La décision K 32/15 du 30 juin 2021

74. En décembre 2015 et en février 2016, le Commissaire aux droits de l'homme polonais a saisi la Cour constitutionnelle, l'invitant à contrôler la constitutionnalité de certaines dispositions de la

législation relative au contrôle opérationnel dans leur rédaction applicable postérieurement à l'entrée en vigueur de la loi du 15 janvier 2016 et de la loi anti-terrorisme. Devant la haute juridiction, il soutenait en particulier que la législation en cause ne mettait pas en œuvre l'arrêt K 23/11 de la Cour constitutionnelle (précité) et que, de surcroît, elle était constitutive de violations encore plus flagrantes des droits et libertés individuels protégés par la Constitution et par les normes de droit international pertinentes que celles sanctionnées par ledit arrêt. Les principaux griefs du Commissaire à cet égard étaient les suivants :

– la durée maximale de surveillance, fixée à dix-huit mois, était excessive et allait au-delà de ce qui était considéré comme « nécessaire dans une société démocratique ». De plus, la législation relative à certains des services de police et de renseignement concernés ne prévoyait aucune limite maximale à la durée d'application de la surveillance ;

– les dispositions énonçant que le tribunal pouvait autoriser l'utilisation des informations couvertes par le secret professionnel comme éléments de preuve dans une procédure pénale dès lors que, selon lui, « l'intérêt de la bonne administration de la justice l'exigeait » étaient entachées d'imprécision et attentatoires aux droits de la défense ;

– la législation attaquée ne garantissait pas au tribunal statuant sur la demande d'autorisation de surveillance un accès à l'intégralité du dossier, puisqu'elle n'imposait pas aux services de l'État sollicitant l'autorisation de surveillance de le soumettre en son entier ;

– le libellé des dispositions précisant la liste des infractions pouvant donner lieu à la collecte de données de communication était trop large ;

– la législation réglementant la collecte de données de communication rendait possible un recours quasi illimité à la mesure en question par les services de l'État, sans le soumettre à un quelconque contrôle externe. Le contrôle exercé par les juridictions régionales sur la base de rapports semestriels transmis par les services de l'État concernés en application de la loi du 15 janvier 2016 n'était pas conforme aux conclusions de l'arrêt K 23/11 de la Cour constitutionnelle et était inefficace, dès lors qu'il était facultatif, que ses conclusions étaient confidentielles et que lesdites juridictions n'étaient pas habilitées à ordonner la destruction des éléments collectés illégalement dans le cadre de la surveillance ;

– les autorités n'avaient pas respecté l'arrêt K 23/11 de la Cour constitutionnelle concernant les points suivants : aucune obligation de notification de la décision de justice ayant autorisé la surveillance à la personne visée n'avait été instaurée, de sorte que celle-ci ne pouvait jamais contester la légalité de pareille mesure ; les différentes catégories de personnes pouvant faire l'objet d'une surveillance étaient insuffisamment précisées ; aucun délai maximal n'avait été fixé relativement à l'application de la mesure de collecte et de traitement des données de communication par les services de l'État ayant diligenté une mesure de ce type et, en outre, la mise en œuvre de la mesure en question par les services de l'État concernés échappait à tout contrôle externe effectif ; l'obligation pour les services de l'ABW, du SKW et ceux du renseignement militaire de procéder à la destruction des données de communication collectées par eux ne s'appliquait qu'aux seules données s'étant révélées sans utilité pour les procédures dans le cadre desquelles elles avaient été collectées ;

– plusieurs dispositions de la loi anti-terrorisme relatives à la surveillance étaient problématiques en raison de leur imprécision et de leur libellé, qui avait une portée trop large.

Tel était tout particulièrement le cas de celles prévoyant la possibilité de recourir à une mesure de surveillance en cas de « soupçons quant à la survenance d'un incident à caractère terroriste ». De plus, la décision du chef de l'ABW en application de laquelle la surveillance était mise en place n'était soumise à aucun contrôle externe.

75. En avril 2017, le Commissaire s'est désisté du premier recours formé par lui, pour autant qu'il visait la durée maximale de la surveillance effectuée par la police nationale, la police des frontières, le service de contrôle fiscal et la police militaire. En mars 2018, le Commissaire a fait de même concernant le second recours déposé, estimant que l'impartialité et la qualité de juge de certaines des personnes participant à la formation de jugement de la Cour constitutionnelle étaient sujettes à caution et qu'en conséquence la formation ainsi constituée n'était pas de nature à garantir un examen indépendant et approfondi de l'affaire, et considérant en outre qu'un éventuel arrêt de la Cour constitutionnelle en la matière pourrait fournir à certains services de l'État concernés un moyen de légitimer leurs pratiques attentatoires aux normes constitutionnelles et européennes applicables.

76. Par la décision K 32/15 du 30 juin 2021, la Cour constitutionnelle a mis un terme à la procédure relative au premier recours du Commissaire, formulant les observations suivantes. Le grief portant sur la durée maximale des surveillances effectuées par l'ABW, le CBA et le SKW était sans objet dès lors que la durée en question avait été ramenée à 12 mois à la suite de l'entrée en vigueur de la loi du 15 janvier 2016. La partie du recours dénonçant des lacunes concernant la procédure d'autorisation du contrôle opérationnel était fondée sur des dispositions de la Constitution inadéquates. Quant au grief relatif à l'absence de notification de la décision de justice ayant autorisé la surveillance aux personnes en faisant l'objet, il concernait une abstention législative, question sur laquelle elle n'avait pas compétence pour statuer, et elle ne pouvait pas par conséquent poursuivre plus avant son examen de ce point.

e) La décision SK 60/21 du 28 juin 2022

77. En mars 2021, une personne ayant fait l'objet d'une surveillance de la part des services de la police nationale a formé une plainte constitutionnelle, arguant que les dispositions de l'article 19 § 20 de la loi sur la police ne prévoyaient aucun recours dans le chef d'un individu soumis à une surveillance contre la décision ayant autorisé celle-ci, et estimant qu'elles étaient par conséquent contraires à la Constitution.

78. Par la décision SK 60/21 du 28 juin 2022, la Cour constitutionnelle a décidé de ne pas poursuivre l'examen de la plainte en question, invoquant des motifs analogues à ceux de la décision K 32/15 (paragraphe 76 ci-dessus).

17. La jurisprudence de la Cour administrative suprême

79. Dans les affaires qui sont exposées ci-après, les plaignants avaient formé des demandes en vue de se voir communiquer des informations quant à l'application des mesures de surveillance secrète par les services de police et de renseignement, invoquant les dispositions pertinentes de la loi sur l'accès à l'information publique. Les responsables desdits services avaient rejeté leurs demandes, indiquant que les éléments d'information sur lesquelles elles portaient étaient classés, et qu'ils ne pouvaient par conséquent leur être communiqués. Les plaignants contestaient les décisions de rejet.

a) L'arrêt I OSK 932/16 du 6 juillet 2017

80. L'arrêt I OSK 932/16 du 6 juillet 2017 concerne le rejet qui avait été opposé par le chef du CBA à la demande formée par la Fondation Helsinki relativement à l'utilisation par les services soumis à la supervision de celui-ci du logiciel Xkeyscore[6]. Écartant les arguments de la fondation plaignante, la Cour administrative suprême a jugé que les informations dont elle sollicitait la communication avaient trait aux méthodes de travail des services de l'État effectuant la surveillance et qu'elles bénéficiaient par conséquent d'une protection analogue à celle applicable aux données classées. Renvoyant aux dispositions pertinentes de l'article 5 de la loi sur la protection des données classées, elle a estimé qu'une communication desdits éléments d'information à la plaignante serait susceptible de nuire à la bonne marche des opérations diligentées par les services du CBA. Elle a indiqué en outre qu'elle était parvenue à cette conclusion après avoir procédé à une mise en balance des impératifs, d'une part, du droit de la plaignante à être informée des activités des pouvoirs publics et, d'autre part, des intérêts économiques de l'État et de la sécurité publique. En marge de ses motifs, elle a ajouté que le principe de transparence de l'action publique ne devait pas être compris comme garantissant la publicité des moyens utilisés par les services de police et de renseignement en vue de la réalisation d'opérations secrètes.

b) L'arrêt I OSK 2248/16 du 18 juillet 2018

81. L'arrêt en question a trait à la demande par laquelle l'ONG Watchdog Polska avait invité le chef de l'ABW à lui communiquer plusieurs éléments d'information concernant une supposée utilisation par les services placés sous sa supervision du système de lecture et de reconnaissance automatique de plaques d'immatriculation. Le chef de l'ABW ayant rendu une décision en sa défaveur, l'intéressée avait saisi le tribunal administratif d'un recours en annulation de celle-ci, lequel avait été rejeté. Dans son jugement, le tribunal administratif avait considéré que bien que l'information dont l'organisation plaignante avait sollicité la communication fût considérée comme « publique », au sens qui était attribué à cette notion par la loi sur l'accès à l'information publique, elle relevait en même temps de la protection prévue à l'article 5 de la loi sur la protection des données classées. Il avait observé en outre qu'en l'occurrence, les éléments d'information en question portaient sur les moyens techniques employés par les services de l'ABW dans l'exercice de leur mission de protection de la sécurité publique, et il avait estimé que leur communication à l'intéressée irait à l'encontre de l'intérêt public. L'association plaignante a contesté ledit jugement devant la Cour administrative suprême. Celle-ci a rejeté le recours, jugeant que les informations sur les moyens utilisés par les services de l'ABW aux fins de l'exécution des missions qui leur étaient dévolues étaient confidentielles en vertu des dispositions pertinentes de la loi sur l'ABW et de la loi sur la protection des données classées. Elle a indiqué en outre que les organismes publics compétents n'étaient pas tenus de fournir des motifs détaillés à l'appui de leurs décisions portant rejet de demandes analogues à celle en cause en l'espèce.

c) L'arrêt I OSK 579/17 du 23 janvier 2019

82. L'affaire en cause dans cet arrêt concernait le refus par le chef de l'ABW de faire droit à la demande d'un individu qui l'avait invité à lui indiquer si les services soumis à sa supervision avaient appliqué des mesures de surveillance à son égard à son insu. Statuant en défaveur du plaignant, la Cour administrative suprême a jugé que, compte tenu de la spécificité des opérations menées par l'ABW et de leurs enjeux pour la sûreté, l'ensemble des informations s'y rapportant, y compris celles relatives aux moyens opérationnels mis en œuvre par les services de l'ABW et à l'existence même d'une mesure de surveillance, devaient rester secrètes. Elle a considéré qu'une communication des éléments d'information en question à l'intéressé pourrait nuire à la bonne marche des opérations réalisées par les services de l'ABW, et elle a estimé par conséquent que le chef de l'ABW ne pouvait fournir au plaignant aucune information relativement à la réalisation supposée d'un contrôle opérationnel le concernant. Elle a ajouté que les informations de ce type, quand bien même elles seraient considérées comme « publiques », n'en étaient pas moins confidentielles en application de l'article 5 § 1 de la loi sur l'accès à l'information publique.

d) L'arrêt I OSK 2687/17 du 27 septembre 2019

83. L'arrêt I OSK 2687/17 du 27 septembre 2019 porte sur un refus opposé par le chef de l'ABW à la demande par laquelle une ONG l'avait invité à lui communiquer des éléments statistiques concernant la surveillance effectuée en application de l'article 9 de la loi anti-terrorisme par les services relevant de sa supervision. A l'appui de sa décision, le chef de l'ABW avait invoqué, entre autres, le caractère confidentiel des informations réclamées par l'organisation plaignante et le risque de voir le succès des opérations menées par ses services en matière de lutte contre le terrorisme compromis dans le cas où elles seraient divulguées. Le tribunal administratif ayant rejeté le recours que l'organisation plaignante avait formé contre la décision en question, l'intéressée s'est pourvue en cassation devant la Cour administrative suprême. Celle-ci a cassé le jugement attaqué et la décision de rejet, renvoyant le dossier au chef de l'ABW en vue de son réexamen. Dans ses motifs, elle a observé que si la communication à l'intéressée d'informations relatives à la fréquence d'application par les services de l'ABW des mesures énoncées aux articles 9 à 11 de la loi anti-terrorisme et au nombre d'individus visés par les mesures en question pouvait compromettre l'efficacité des services de l'État concernés, les motifs avancés par le chef de l'ABW n'avaient pas justifié qu'il en allât de même des informations sur la fréquence d'utilisation par lui des attributions qui lui étaient dévolues en application de l'article 11 § 1 de la même loi. Elle a indiqué qu'il ne faisait aucun doute à ses yeux qu'une divulgation par le chef de l'ABW d'informations du premier type à l'intéressée serait susceptible de nuire à la sécurité nationale, à l'ordre public et à la bonne marche des opérations diligentées par les services soumis à sa supervision, ce qui impliquait que lesdites informations devaient rester confidentielles. Elle a précisé que, considérés dans un contexte analogue, même des éléments d'information purement statistiques sur la pratique en matière de surveillance des services de l'État concernés pouvaient parfois apparaître comme sensibles pour la sûreté et être soumis à une protection accrue, équivalente à celle applicable aux informations confidentielles. Elle a ajouté qu'en pareille situation, la divulgation d'informations de ce type à quiconque serait prohibée en application de l'article 5 de la loi sur l'accès à l'information publique.

C. Les données statistiques pertinentes

84. Chacune des parties a produit des éléments statistiques sur l'application de la surveillance secrète par les services de l'État au cours de la période allant de 2017 à 2022. Les éléments d'information en question sont issus principalement des rapports annuels établis respectivement par le procureur en chef du parquet national, par le ministre de l'Intérieur et par le ministre de la Justice à l'attention du Parlement. Les rapports du procureur en chef du parquet national se réfèrent au nombre d'individus visés par des demandes d'autorisation de surveillance, et ceux du ministre de l'Intérieur comptabilisent le nombre de demandes d'autorisation soumises aux tribunaux. Les documents communiqués indiquent ce qui suit :

Année	Nombre d'individus visés par des demandes d'autorisation de surveillance	Nombre d'individus pour lesquels une demande d'autorisation de mise sur écoute ou de contrôle opérationnel a été rejetée par procureur	Nombre d'individus pour lesquels un procureur a approuvé les demandes d'autorisation de surveillance	Nombre d'individus pour lesquels un tribunal a rejeté une demande d'autorisation de mise sur écoute ou de contrôle opérationnel	Nombre d'individus pour lesquels un tribunal a autorisé une mise sur écoute ou de contrôle opérationnel	Pourcentage d'individus pour lesquels un tribunal a autorisé une mise sur écoute et un contrôle opérationnel	Pourcentage d'individus pour lesquels un procureur ou un tribunal a autorisé une mise sur écoute et un contrôle opérationnel
2021	7071	126	6945	25	6922	97,8 %	99,66 %
2020	6537	118	6419	35	6384	97,65 %	99,45 %
2019	5839	103	5736	25	5711	97,81 %	99,56 %
2018	6088	148	5940	25	5915	97,16 %	99,58 %
2017	6562	146	6416	14	6402	97,56 %	99,78 %

Année	Nombre de demandes de surveillance soumises pour autorisation	Nombre de demandes d'autorisation de surveillance rejetées par un procureur	Nombre de demandes d'autorisation de surveillance approuvées par un procureur	Nombre de demandes d'autorisation de surveillance rejetées par un tribunal	Nombre de demandes d'autorisation de surveillance approuvées par un tribunal	Nombre de dossiers dans lesquels les éléments collectés au moyen de la surveillance ont été utilisés comme éléments de preuve dans une procédure pénale	Pourcentage de dossiers dans lesquels un tribunal a autorisé une mise sur écoute et un contrôle opérationnel	Pourcentage de dossiers dans lesquels un procureur ou un tribunal a accepté une demande de mise sur écoute ou de contrôle opérationnel	Pourcentage de dossiers dans lesquels les éléments collectés dans le cadre d'une surveillance ont été utilisés comme éléments de preuve
2017	9879	142	9734	9	9725	1525	98,47 %	99,91 %	15,68 %
2018	8451	205	8246	8	8238	1730	97,48 %	99,90 %	21 %
2019	8199	116	8083	15	8068	1303	97,48 %	99,81 %	16,15%
2020	10115	150	10005	21	9984	1471	99,79 %	99,79 %	14,73 %
2021	11074	155	10919	7	10912	1672	99,93 %	99,93 %	15,32 %

85. Il ressort des éléments d'information communiqués par le Gouvernement, lesquels n'ont pas été remis en cause par les requérants, qu'au cours de la période comprise entre 2017 et 2021, la police a eu recours au contrôle opérationnel principalement en vue de la prévention ou de la découverte d'infractions à l'ordre public, à la vie et la santé, à la sûreté et à la liberté individuelle, d'infractions contre les biens, les institutions de l'État et les autorités locales, du commerce de devises et de titres financiers, des transactions commerciales ainsi que des infractions à la loi sur la lutte contre les stupéfiants.

86. Les éléments d'information annuels réunis par le ministre de la Justice à l'attention du Parlement indiquent le nombre de fois où les services de l'État compétents ont procédé à la

collecte de données de communication. Il en ressort en outre que sur 107, 163 et 136 contrôles de l'application de la mesure de surveillance en question réalisés par les tribunaux au cours de la période comprise entre 2019 et 2021, respectivement un seul et deux ont abouti à une évaluation en défaveur des services de l'État concernés par les contrôles en question.

Année	Données liées aux télécommunications	Données liées aux communications postales	Données liées aux communications en ligne
2021	1 820 630	16 764	20 107
2020	1 546 326	13 309	24 959
2019	1 345 207	8 595	19 526
2018	1 325 241	8 601	22 933
2017	1 227 314	13 630	23 913

II. LES TEXTES INTERNATIONAUX PERTINENTS

A. Nations unies

La résolution no 68/167 sur le droit à la vie privée à l'ère du numérique

87. La résolution no 68/167 sur le droit à la vie privée à l'ère du numérique, adoptée par l'Assemblée générale le 18 décembre 2013, est ainsi libellée en ses passages pertinents en l'espèce :

« L'Assemblée générale,

(...)

4. Invite tous les États :

(...)

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

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

(...) »

B. Conseil de l'Europe

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

88. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel énonce des normes en matière de protection des données dans le

domaine du traitement automatique des données à caractère personnel dans les secteurs public et privé. En ses parties pertinentes en l'espèce, elle prévoit ce qui suit :

Préambule

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

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

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

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

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

Sont convenus de ce qui suit : »

Article 1er - Objet et but

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

(...) »

Article 8 -Garanties complémentaires pour la personne concernée

« Toute personne doit pouvoir :

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

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

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

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

Article 9 – Exceptions et restrictions

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

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

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

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

(...) »

Article 10 - Sanctions et recours

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

89. Le rapport explicatif de ladite convention expose notamment ce qui suit :

Article 9 - Exceptions et restrictions

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

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

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

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

2. *Le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (8 novembre 2001, STCE no 181)*

90. Les dispositions pertinentes en l'espèce du Protocole additionnel du 8 novembre 2001 se lisent ainsi :

Article 1 – Autorités de contrôle

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

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

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

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

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

(...) »

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

91. La recommandation no R (95) 4 du Comité des Ministres, adoptée le 7 février 1995, énonce ce qui suit en ses parties pertinentes en l'espèce :

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

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

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

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

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

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

c. la conservation ou la destruction de ces données.

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

4. *Le rapport de la Commission européenne pour la démocratie par le droit (« Commission de Venise ») relatif à la loi du 15 janvier 2016 portant modification de la loi sur la police et certaines autres lois*

92. Les passages pertinents de l'avis sur le projet de loi relatif à la loi du 15 janvier portant modification de la loi sur la Police et de certaines autres lois, adopté par la Commission de Venise lors de sa 107e session plénière, (Venise, 10-11 juin 2016, CDL-AD (2016)012) se lisent ainsi :

« II. Portée de l'analyse

5. Les amendements de 2016 visaient à codifier des méthodes de surveillance secrète employées par les services de police et de renseignement. Des organismes de l'État peuvent obtenir de l'information de multiples façons : témoins ou informateurs, fouilles et perquisitions de locaux, surveillance « classique » (filatures), etc. Mais ce qui avait surtout attiré l'attention publique et les critiques, c'était le pouvoir donné aux organismes de l'État d'obtenir de l'information par surveillance des moyens de communication et d'autres appareils ou canaux : ordinateurs, téléphones, banques de données, courrier électronique, réseaux sociaux, etc. C'est pourquoi la Commission de Venise se penche dans son analyse sur les dispositions de la loi relatives à ces modes de surveillance.

6. Le présent avis envisage les actions « normales » des services de répression, c'est-à-dire la surveillance exercée dans un but de lutte contre la criminalité à l'intérieur du pays. La Commission de Venise n'analyse pas ici les activités de surveillance des services de renseignement extérieur, des services militaires de contre-espionnage, etc. Elle n'en a pas moins conscience que la distinction est floue entre la surveillance normale pratiquée au titre de la répression des infractions et le renseignement mené dans un but de sécurité nationale. Mais le renseignement est un domaine extrêmement complexe et délicat, qui mérite une analyse à part.

7. Les modifications de 2016 concernaient plusieurs lois portant sur les activités de services de police et de renseignement. Tous ces textes prévoient en fin de compte le même modèle de surveillance (à quelques petites exceptions près). La Commission de Venise se concentre ici sur la loi sur la police, qui pourra servir d'exemple, *mutatis mutandis*, pour les normes relatives à d'autres organismes. »

III. Contexte des modifications apportées à la loi sur la police et à d'autres textes

« 10. Les modifications visaient à mettre le système juridique polonais en conformité avec l'arrêt K 23/11 du 30 juillet 2014 du Tribunal constitutionnel de Pologne (...)

11. Soucieux d'éviter un vide juridique, le Tribunal constitutionnel avait donné au législateur 18 mois (soit jusqu'au 7 février 2016) pour modifier les textes concernés. Mais les modifications nécessaires n'ayant pas pu être apportées au cours de la législature précédente, le nouveau Parlement formé au mois de novembre 2015 a eu peu de temps pour mettre en œuvre l'arrêt du 30 juillet 2014. Les modifications ont finalement été adoptées dans le cadre d'une procédure accélérée. »

IV. Brève description de la loi sur la police

« 12. Les paragraphes suivants reprennent brièvement les dispositions concernées de la loi sur la police après modification. La Commission de Venise se concentrera sur deux d'entre elles : l'article 19 (sur la surveillance « classique »), et l'article 20c (sur la collecte de métadonnées – terme dont le sens est expliqué au paragraphe 15).

13. L'article 19 contient les règles relatives à la surveillance secrète (désignée par *operational control*, « contrôle opérationnel », dans la traduction anglaise officielle de la loi sur la police) ordonnée dans le cadre des enquêtes préliminaires sur une affaire concernant des infraction (potentielles) énumérées aux alinéas 1 à 8 du paragraphe 1. Il a été expliqué aux rapporteurs de la Commission de Venise à Varsovie que la surveillance secrète prévue à l'article 19 n'est pas soumise aux règles formelles de recherche des éléments de preuve figurant dans le Code de procédure pénale : il s'agirait de deux régimes juridiques distincts. La surveillance secrète précède fréquemment, pour la justifier, l'ouverture d'une enquête. Mais toute surveillance secrète ne débouche pas sur l'ouverture d'une procédure pénale. En revanche, les informations obtenues par surveillance secrète peuvent être présentées comme éléments de preuve dans les procédures pénales. La surveillance secrète est ordonnée pour une durée maximale de trois mois (paragraphe 8), mais peut être prolongée jusqu'à 18 mois (paragraphe 9).

14. Le paragraphe 6 de l'article 19 fait relever de la surveillance secrète des mesures comme les écoutes, l'enregistrement du contenu de conversations téléphoniques et de la correspondance empruntant les réseaux de télécommunications (e-mails, messageries, etc.), ainsi que l'interception de la correspondance postale, l'enregistrement sur le vif de conversations à l'aide de dispositifs appropriés, etc. Ce qui veut dire que la surveillance secrète « classique » que prévoit l'article 19 permet à la police de connaître le contenu de communications que les interlocuteurs croyaient confidentielles.

15. L'article 20c de la loi sur la police traite des métadonnées. Pour dire les choses simplement, il s'agit de toutes les données liées aux communications et télécommunications et les concernant. Elles peuvent englober des informations sur les appels téléphoniques effectués ou reçus, les numéros composés, la durée des appels, la localisation géographique des appareils mobiles à tel ou tel moment, les sites Internet consultés, les connexions à des sites, les paramètres personnels, les adresses de correspondance e-mail, etc. L'accès aux métadonnées ne livre pas le contenu des communications privées (article 20c, paragraphe 1), en tout cas pas de la même façon que la surveillance « classique » relevant de l'article 19. Pourtant, comment on le verra ci-dessous, la distinction entre le contenu et sa forme n'est plus aussi claire, et les métadonnées peuvent véhiculer une information considérable sur la vie privée d'une personne. Le sens du terme est encore précisé dans la législation afférente (loi sur les télécommunications, loi sur les services électroniques et loi sur la poste).

16. La surveillance secrète de l'article 19 et la collecte de métadonnées de l'article 20c diffèrent par les motifs pour lesquels elles sont ordonnées et par leurs procédures. En ce qui concerne les motifs, l'article 19 contient une liste exhaustive d'infractions justifiant la surveillance. L'article 20c prévoit un cadre juridique beaucoup plus large pour la collecte de métadonnées, qui est demandée pour prévenir ou détecter des infractions, sauver des vies et préserver la santé humaine, ou à l'appui d'opérations de recherche et de sauvetage. En définitive, la police

peut collecter des métadonnées à toute fin utile à sa mission très largement comprise de maintien de l'ordre et de la paix.

17. Au niveau procédural, la surveillance secrète régie par l'article 19 nécessite généralement l'autorisation préalable d'un tribunal de district (paragraphes 1 et 2). Mais dans les cas d'extrême urgence, où tout retard pourrait se traduire par une perte d'informations ou encore la destruction ou la disparition d'éléments de preuve d'une infraction, la police peut entamer la surveillance sans l'autorisation préalable du tribunal, moyennant celle du procureur. Si l'autorisation n'est pas accordée dans les cinq jours, la surveillance doit être suspendue et les informations recueillies détruites (paragraphe 3).

18. En revanche, l'article 20c permet d'obtenir des métadonnées sans autorisation préalable de justice. L'article 20ca ne prévoit qu'un système de contrôle *a posteriori* : tous les six mois, la police est tenue de soumettre pour contrôle au tribunal compétent un rapport général sur la collecte de métadonnées (paragraphe 2). Enfin, l'article 20cb contient les règles de traitement et d'obtention de certaines données non soumises à quelque contrôle que ce soit, même *a posteriori*. En fin de compte, la loi sur la police met en place deux régimes juridiques fondamentalement différents : l'un pour la surveillance secrète « classique » des communications, et l'autre pour la collecte des métadonnées.

19. Il semble que la collecte des métadonnées prévue à l'article 20c est une technique d'enquête très utilisée, alors que la surveillance secrète « classique » des communications est beaucoup plus rare. Le ministère de l'Intérieur indique qu'en 2015, la police a enquêté sur 833 361 affaires, dont 215 561 portaient sur des infractions figurant dans la liste du paragraphe 1 de l'article 19. Dans ce groupe, la surveillance secrète a été ordonnée 8 000 fois (soit 0,9 % du total d'affaires en instance, et 3,7 % des affaires figurant dans la liste du paragraphe 1 de l'article 19). Le procureur a refusé la surveillance à la police dans 178 cas, et les tribunaux dans 19.

20. En ce qui concerne la collecte de métadonnées, des organismes de répression ont déposé 1 497 174 demandes en 2015, dont 1,3 million portant sur des données de télécommunications, et 0,2 million sur des données Internet. Dans ce dernier cas, les demandes concernaient notamment des adresses www (902 fois) ainsi que des adresses e-mail, des outils de communication sur l'Internet, des blogs et des chats (4 913 fois). Les factures détaillées (contenant des renseignements sur les numéros appelés, avec date, heure et durée de l'appel) sont l'information le plus souvent demandée (703 819 fois en 2015). Quelque 330 000 demandes portaient sur des données moins sensibles (nom et adresse de l'utilisateur abonné d'un appareil de communication). La Commission de Venise rappelle que la Pologne possède une population de plus de 38 millions d'habitants.

21. (...) la Commission de Venise souligne que les modifications de 2016 apportent plusieurs améliorations au système. Par exemple, la loi précise à présent les moyens de surveillance secrète (article 19, paragraphe 6), elle couvre les interventions techniques et fixe la durée maximale de la surveillance secrète lorsqu'elle est prolongée (paragraphe 9 de l'article 19) ; la loi sur la police fait obligation à cette dernière de journaliser les opérations de surveillance secrète (paragraphes 16a et 16b de l'article 19) ; elle met en place une procédure de contrôle juridictionnel *a posteriori* de la collecte de métadonnées (article 20ca) ; elle prévoit la destruction ou des restrictions d'utilisation des informations couvertes par le secret professionnel et

obtenues par surveillance (paragraphes 15 et suivants de l'article 19) ; elle donne une description plus détaillée des pouvoirs des services associés à la collecte de métadonnées de l'Internet (articles 20c et suivants), et impose la destruction des données non pertinentes (paragraphe 7 de l'article 20c).

31. (...) La Commission de Venise constate que les données collectées en application de l'article 20c de la loi peuvent permettre de connaître les relations sociales de la personne, ses habitudes, ses préférences et ses centres d'intérêt. L'analyse combinée de divers types de métadonnées (que n'interdit pas la loi) et le traitement d'un important volume de renseignements ainsi obtenus peuvent constituer une ingérence encore plus profonde et révéler des aspects intimes de la vie privée d'une personne. Ces données collectées secrètement par les services de répression peuvent être utilisées dans une procédure pénale contre ladite personne ou d'autres. Le législateur polonais ferait donc une hypothèse plus plausible en partant du principe que la collecte de la plupart des types de métadonnées en vertu de l'article 20c de la loi constitue une ingérence dans la vie privée de la personne concernée.

(...) »

1. Motifs matériels de mise en place d'une surveillance en vertu de l'article 19

a. Les infractions qui justifient la surveillance secrète et le principe de proportionnalité dans ce contexte

« 39. L'article 19 de la loi contient une liste exhaustive des infractions pouvant donner lieu à une surveillance secrète, ce qui clarifie le champ d'application matériel de cette disposition. La liste du paragraphe 1 est toutefois très ample. La Commission de Venise rappelle que (...) eu égard à l'ingérence qu'elle représente, la surveillance secrète du contenu des communications à caractère privé n'est justifiée que pour des infractions graves. En ce qui concerne la loi sur la police, la Commission de Venise doute, par exemple, que des écoutes téléphoniques soient nécessaires dans certaines affaires de possession illégale de substances psychotropes (article 19, paragraphe 1, alinéa 5) dès lors qu'il est d'emblée évident qu'il s'agit de quantités très modestes destinées à l'usage personnel.

40. La Commission de Venise répète que certaines mesures de surveillance prévues au paragraphe 6 de l'article 19 constituent non seulement une ingérence dans la confidentialité des communications à caractère privé, mais aussi une ingérence dans le respect du domicile (la loi autorise la mise sur écoute de bureaux ou de locaux à usage d'habitation). Ce type de surveillance doit être très solidement justifié et n'être admissible que dans les enquêtes sur les infractions les plus dangereuses (...)

41. La Commission de Venise n'en reconnaît pas moins que les autorités polonaises disposent d'une large marge d'appréciation en ce qui concerne les infractions à inscrire sur cette liste, la question relevant dans une large mesure des priorités politiques nationales en matière pénale.

42. Plus important encore : la loi devrait mentionner explicitement le principe de proportionnalité. Elle en évoque déjà certains éléments ; l'article 19 définit par exemple les mesures de surveillance comme un instrument auxiliaire d'enquête (voir paragraphe 46). Et elle contient une liste exhaustive des infractions pouvant donner lieu à une surveillance. Mais

la proportionnalité ne saurait se réduire à cela. Il devrait être exigé de tous les acteurs impliqués – police comme tribunaux – qu'ils apprécient en l'espèce si la gravité de l'infraction (quand bien même elle figurerait dans la liste du paragraphe 1 de l'article 19) et la complexité de l'enquête requièrent une quelconque mesure de surveillance. La réponse peut être évidente pour les infractions les plus graves, mais toutes celles qui figurent sur la liste n'appelleraient pas automatiquement une surveillance (surtout s'il s'agit d'une ingérence dans le respect du domicile), et le texte de la loi devrait clairement l'indiquer. »

b. Nécessité d'une justification factuelle

« 43. La liste du paragraphe 1 de l'article 19 énumère les types d'infractions sur lesquels la police peut enquêter par surveillance secrète. Mais ce critère est purement formel, puisqu'il repose sur la façon dont la police qualifie une situation concrète appelant une enquête. Or la police peut se tromper dans son évaluation des faits, ou leur donner délibérément une étiquette juridique les faisant relever de l'article 19 (...). Par conséquent, outre la nécessité de s'assurer que l'infraction pour laquelle la police demande une autorisation en application du paragraphe 2 de l'article 19 figure bien dans la liste du paragraphe 1 du même article, le tribunal devrait aussi examiner les éléments de preuve concrets déjà réunis, et décider sur cette base si la surveillance secrète se justifie.

(...)

44. (...) La loi n'en devrait pas moins spécifier clairement que pour procéder à une surveillance, la police et le procureur doivent posséder au moins quelques prima facie éléments de preuve d'une activité criminelle, au vu desquels le tribunal décidera d'autoriser ou non la surveillance

c. Probabilité d'obtention d'informations importantes par surveillance

45. La police devrait avoir des raisons suffisantes de présumer que la surveillance de la personne ou du groupe qui en feront l'objet fournira des informations utiles à l'enquête (...) une telle affirmation doit être étayée par certains faits et indices.
(...) »

e. Valeur probante de l'information

« 47. (...) la loi sur la police ne dit rien de la valeur probante des informations obtenues par une surveillance secrète qui se révèle avoir été ordonnée sans justification suffisante. On ne voit pas très bien si les enregistrements, images, etc. ainsi recueillis sont utilisables dans une procédure pénale (...)

48. On ne sait (...) pas vraiment dans quelle mesure ces renseignements sont utilisables lorsque l'autorisation a été obtenue, mais sur la base de motifs insuffisants. La Commission de Venise rappelle que la procédure d'autorisation aura lieu à huis clos dans la plupart des cas, et que ni le public, ni la personne concernée, ne sauront si la juridiction chargée de la décision avait convenablement tenu compte de l'impératif de protection de la vie privée. En pareil cas, le tribunal examinant l'affaire sur le fond devrait pouvoir exclure à sa discrétion les éléments de preuve obtenus par surveillance secrète que présente le ministère public s'il y a eu violation grave et flagrante de la loi, dans un souci de lutte contre les abus de surveillance. »

2. Motifs matériels de collecte de métadonnées en vertu de l'article 20c de la loi sur la police

a. Infractions justifiant la collecte de métadonnées

« 49. La police dispose d'une discrétion beaucoup plus large en ce qui concerne la collecte de métadonnées, autorisée si elle sert à prévenir ou à détecter des activités criminelles, à sauver des vies humaines ou à protéger la santé, ou encore dans des opérations de recherche et de sauvetage (paragraphe 1 l'article 20c de la loi sur la police) (...)

53. (...) L'article 20c de la loi sur la police (...) autorise la collecte de métadonnées dans les enquêtes portant sur toutes les infractions. Il est par ailleurs raisonnable de penser que la collecte de données autorisée par l'article 20c de la loi peut à l'occasion se traduire par des ingérences plus graves dans la vie privée que la surveillance par GPS sur une durée relativement brève des déplacements d'une automobile – par exemple s'il y a analyse de métadonnées se rapportant au contenu (comme la journalisation des sites Web).

54. (...) Il ne semble pas que la formulation large de l'article 20c (à savoir que la police peut recourir à la collecte de métadonnées pour prévenir ou détecter des infractions) satisfasse à l'exigence de prévisibilité posée à l'article 8 de la CEDH. Une façon de limiter les possibilités d'abus de ce mode d'investigation serait d'indiquer que la collecte de métadonnées n'est admissible que dans les enquêtes portant sur des infractions passibles d'une peine minimum donnée. Il serait possible de compléter la disposition par une liste plus courte d'infractions non soumises à la règle de la peine minimum, mais pour lesquelles la collecte de métadonnées constitue tout ou partie des preuves essentielles du ministère public, comme, par exemple, certaines formes de cybercriminalité. Il y aurait donc des façons plus appropriées d'éviter les risques que suscite la formulation très large de la loi. La Commission de Venise invite le législateur polonais à envisager de restreindre la portée de la règle actuellement formulée à l'article 20c de la loi. »

b. Probabilité d'obtention d'informations importantes par collecte de métadonnées

« (...)

56. L'article 20c n'indique aucun critère de probabilité auquel la police doit satisfaire pour recueillir des métadonnées. La Commission de Venise pense qu'il est essentiel que la police possède des raisons spécifiques de juger :

– qu'une infraction a été commise, ou qu'une activité criminelle est en cours ou en préparation ;

– et que la surveillance permettra vraisemblablement d'en savoir plus à ce sujet.

Ce qui veut dire que la police devrait être en mesure d'expliquer, en s'appuyant sur des faits, en quoi la collecte de métadonnées contribuera à l'enquête menée sur une activité criminelle donnée. »

c. Subsidiarité

« 57. La Commission de Venise constate que, contrairement au cas de la surveillance secrète prévue à l'article 19 de la loi, la loi polonaise ne donne pas statut subsidiaire à la collecte de

métadonnées parmi les modes de recherche d'informations.
58. (...) La loi n'exige pas que d'autres méthodes aient été précédemment utilisées sans résultat, ou ne soient pas utilisables, ce qui renforce la nécessité de mettre en place des garanties contre l'abus de cet instrument par les services de répression et de sécurité (...)

59. La loi devrait par ailleurs contenir une règle indiquant sur le plan matériel à la police quand elle peut recourir à cette méthode. (...) la police ne devrait le faire que lorsque cela est dûment justifié, même pour les métadonnées les moins sensibles. Il est indispensable de s'interroger sur les critères de contrôle que devront appliquer les tribunaux pour déterminer si la police a agi dans les limites de la loi et de son pouvoir discrétionnaire. Le critère devrait être plus strict s'il s'agit de surveillance secrète de contenus : la police devrait être tenue de démontrer dûment qu'il lui serait impossible d'obtenir l'information par d'autres moyens, et que les renseignements à réunir ainsi sont essentiels. En revanche, pour ce qui est des métadonnées, le tribunal pourrait admettre qu'il s'agit de la méthode la plus aisée pour obtenir l'information dans les circonstances de l'espèce, et que ces renseignements sont raisonnablement en rapport avec les buts de l'enquête. Il appartient au législateur polonais de formuler la règle qui différenciera le critère de probabilité suivant qu'il s'agit de la surveillance secrète ou de la collecte de métadonnées. »

d. La notion de métadonnées à l'article 20c

« 60. Il reste à s'interroger sur la nature de l'information que l'article 20c permet de collecter. La loi elle-même ne décrit pas précisément ce qu'il faut comprendre par métadonnées, mais renvoie à plusieurs autres textes relatifs aux télécommunications, à l'Internet et aux services postaux (...). Il revient aux spécialistes des domaines concernés de dire si les termes techniques qui y figurent décrivent les métadonnées avec une précision suffisante. (...)

61. La Commission de Venise commence par constater que les métadonnées « ne constituent pas un message de télécommunication » (loi sur la police, paragraphe 1 de l'article 20c). Cela voudrait dire que, dans la logique du texte, les métadonnées ne doivent pas révéler le contenu d'une communication au sens strict. Mais lors des entretiens qu'ils ont eus à Varsovie, les rapporteurs ont reçu des réponses contradictoires à la question de savoir si, en droit polonais, les métadonnées englobent les informations se rapportant au contenu : journalisation des consultations Web, cookies, contenu des recherches, en-tête des e-mails, etc. La Commission de Venise pense que la loi devrait soit établir un lien entre ce type de métadonnées et le contenu des communications, dont l'accès est régi par l'article 19, soit l'exclure explicitement des métadonnées. Il importe de faire cette distinction pour déterminer le degré de rigueur des garanties procédurales et des règles matérielles applicables aux métadonnées se rapportant au contenu.

62. Deuxièmement, le paragraphe 2 de l'article 180c de la loi sur les télécommunications charge les ministres compétents, dont le ministre de l'Intérieur, de fixer par voie d'ordonnance la liste détaillée de données mentionnées au paragraphe 1 de l'article 180c et que la police peut collecter en vertu de l'article 20c. Il est très important de veiller à ce que ce pouvoir de réglementation de ce domaine par ordonnance ne se traduise pas par un élargissement incontrôlé de la notion de métadonnées. (...)

63. Troisièmement, l'article 20c renvoie également à l'article 180d de la loi sur les télécommunications, qui renvoie lui-même à l'article 161.1 du même texte. Ce dernier prévoit que le fournisseur de services de TIC offerts au public peut, moyennant le consentement de l'utilisateur s'il s'agit d'une personne physique, traiter d'autres données (...) de l'utilisateur liées au service qui lui est fourni. Cette formulation semblerait signifier que les métadonnées peuvent englober toutes les informations que l'abonné d'un service de TIC répandu a consenti à partager avec son fournisseur de service. Or on sait que peu d'utilisateurs lisent toutes les clauses d'un contrat de fourniture définissant l'information qu'ils partagent « de leur plein gré » avec le fournisseur pour bénéficier du service. Lue en combinaison avec l'article 20c de la loi, cette disposition peut donc conduire à un élargissement pratiquement incontrôlé des catégories de métadonnées que peuvent collecter les fournisseurs de services TIC, et en fin de compte le gouvernement. Cette approche n'est pas non plus compatible avec le principe de la libre disposition des données, qui fait partie intégrante de la vie privée (...).

(...)

65. La Commission de Venise recommande donc au législateur polonais de vérifier, si nécessaire avec l'appui de professionnels des TIC et de juristes spécialisés dans les domaines concernés, si la description des métadonnées qui figure dans la législation circonscrit suffisamment les catégories d'informations que l'article 20c permet de collecter. Une attention particulière serait de mise en ce qui concerne les données se rapportant au contenu. La Commission de Venise recommande à cet égard d'éviter les formules non limitatives, ou celles qui renvoient à des règles définies par le pouvoir exécutif ou aux politiques des prestataires de services TIC en matière de données. »

C. Personnes sujettes à la surveillance et à la collecte de métadonnées

1. Groupes nombreux

« (...)

69. Pour ce qui est de la collecte de métadonnées (article 20c), (...) rien dans la loi ne semble s'opposer à ce que la police en collecte sans ciblage (...)

70. (...) De l'avis de la Commission de Venise, une surveillance de ce type est admissible sans décision de justice si la loi contient des garanties suffisantes de protection contre l'interception sans discrimination de gros volumes de communications. Pour réduire ce risque, la loi devrait décrire les situations dans lesquelles une surveillance largement ciblée est autorisée, et préciser les catégories de personnes dont les communications sont susceptibles d'être surveillées. Les exigences à satisfaire pour l'autorisation de ce type de surveillance devraient être strictes (enquêtes menées sur de graves infractions spécifiques déjà commises, par exemple). Il pourrait être exceptionnellement possible de permettre la prévention de dangers concrets à venir, comme des menaces terroristes.

71. Si l'autorisation est donnée, le contrôle doit impérativement être très robuste. Un système efficace de supervision de ces mesures devrait être en place et confié à un organe indépendant (ou plusieurs) n'appartenant pas à la police. Cet organe devrait avoir accès aux documents justifiant la surveillance et aux résultats de cette dernière. Il devrait avoir pour mission de garantir en particulier qu'une surveillance largement ciblée est raisonnablement

proportionnée aux besoins d'une enquête particulière, sans motif discriminatoire (elle ne doit pas cibler les groupes de population souvent soupçonnés de commettre certaines infractions), qu'il n'y est jamais recouru à des fins étrangères à la mission de la police ou du service de répression concerné, et que toutes les informations non nécessaires à l'enquête concernée sont systématiquement détruites. »

2. Personnes non soupçonnées

« 72. La loi n'indique pas tout à fait clairement qui peut être soumis à une surveillance secrète « classique » ou à la collecte de métadonnées. Ce peut être, semble-t-il, n'importe quelle personne ou groupe (amis, proches, etc. de la personne ciblée) pour autant que l'on puisse probablement obtenir ainsi des informations qui permettraient d'atteindre les buts définis à l'article 29 pour la surveillance et à l'article 20c pour la collecte de données.

73. La Commission de Venise pense que le principe de prévisibilité impose que la loi définisse plus précisément la nature de l'implication des personnes ou groupes concernés dans l'activité illicite faisant l'objet de l'enquête. Il y a bien sûr d'abord les personnes directement soupçonnées. Mais la loi pourrait en outre mentionner que d'autres personnes en contact avec les premières peuvent, dans certains cas, être soumises à la surveillance. (...) il est très important que la loi décrive les situations dans lesquelles peuvent être ciblées des personnes qui ne sauraient raisonnablement être considérées comme directement associées à une activité criminelle. Elle pourrait par exemple admettre des mesures de ce type uniquement pour des infractions particulièrement graves (terrorisme, trafic de stupéfiants à grande échelle, prolifération d'armes de destruction massive, etc.) et exiger une justification renforcée (probabilité plus forte d'obtention d'informations essentielles par ce moyen) et des garanties procédurales plus strictes (comme l'implication d'un « avocat de la vie privée »).

74. Au cours de leur visite à Varsovie, les rapporteurs ont appris que le Code de procédure pénale avait été modifié en avril 2016, et que les paragraphes 15a à 15e de l'article 19 de la loi sur la police avaient été abrogés. Ces modifications donneraient au procureur discrétion pour décider si l'information obtenue par accident sur une personne non ciblée par une surveillance peut être utilisée dans une procédure pénale engagée contre elle. La Commission de Venise considère que l'utilisation d'une information ainsi obtenue sur une tierce personne comme preuve à charge ne doit être qu'exceptionnellement admissible, et par décision de justice. Elle ne devrait probablement pas être déclarée admissible dans des poursuites pour des infractions relativement mineures. La Commission de Venise considère également que la loi doit absolument préciser clairement les cas dans lesquels de telles informations ne peuvent pas servir de preuve – par exemple si des conversations accidentellement interceptées et enregistrées sont couvertes par le secret professionnel. »

3. Avocats, prêtres et autres personnes bénéficiant de la protection du secret professionnel

« (...)

77. La Commission de Venise relève deux lacunes majeures dans les dispositions relatives à la surveillance des communications couvertes par le secret professionnel. La première concerne le secret des communications entre l'avocat et son client. La loi prévoit bien ce qu'il doit advenir

de l'information couverte par le secret professionnel déjà obtenue par surveillance secrète, mais elle ne semble pas interdire la surveillance des communications des avocats en soi. Rien n'empêche la police de mettre sur écoute secrète les conversations entre un avocat de la défense et son client. Cela n'est pas acceptable aux yeux de la Commission de Venise, pour les raisons expliquées ci-dessous.

78. L'interdiction d'utiliser dans une procédure pénale comme élément de preuve contre un suspect l'information obtenue en violation du secret professionnel et l'obligation de la détruire (article 15f) ne suffisent pas. En écoutant les conversations entre l'avocat et son client, la police peut obtenir des informations importantes, qui la conduiront à d'autres preuves à charge qu'elle pourrait produire dans une procédure pénale. Même si dans la procédure pénale polonaise, ces preuves, « fruits de l'arbre empoisonné », ne sont pas admissibles, l'écoute des conversations entre l'avocat et son client donne à la police un avantage tactique et mine la confiance qui doit régner entre l'avocat de la défense et l'accusé.

79. Pour la Commission de Venise, la loi devrait distinguer la violation délibérée (qui devrait être en général interdite) ou accidentelle du secret. Dans certaines situations évidentes, la police devrait présumer que la conversation est couverte par le secret professionnel (entretiens entre l'avocat et son client à la prison ou dans la salle d'audience, consultations téléphoniques, etc.). L'écoute de ces communications devrait en principe être interdite (...)

80. La présomption ci-dessus n'est pas absolue. (...) Mais une dérogation n'est possible que dans des cas exceptionnels, par exemple s'il existe des signes fiables que l'avocat est personnellement et consciemment associé à une infraction particulièrement grave et que l'écoute de ses conversations avec son client constitue la seule méthode d'investigation possible dans la suite de l'enquête. Cette dérogation devrait être flanquée de garanties procédurales renforcées (l'écoute sera par exemple confiée à un magistrat indépendant qui n'aura aucun lien avec l'instruction et sera tenu au secret sur les informations non pertinentes dont il prendra ainsi connaissance).

81. La seconde lacune porte sur l'interception des communications d'autres professionnels également tenus au secret de leurs communications avec leurs clients (comme les médecins et les médiateurs). La Commission de Venise constate que, comme dans le cas des avocats et des prêtres, rien dans la loi polonaise n'empêche la police d'écouter leurs conversations, même si l'enregistrement ne peut pas ensuite être utilisé comme preuve. Le paragraphe 15h de l'article 19 impose en outre au tribunal d'admettre ces enregistrements comme preuve « si cela est nécessaire dans la perspective du système judiciaire » et s'il n'existait aucun autre moyen d'établir les faits.

82. La seconde partie de l'exigence de subsidiarité est saine ; mais sa première partie (« nécessité » pour la justice) fait problème. Toute information permettant de faire la lumière sur une affaire peut être considérée comme « nécessaire dans la perspective du système judiciaire ». Si l'utilité est le seul critère d'admissibilité d'une conversation interceptée comme preuve, le secret professionnel perd tout son sens.

(...)

84. La Commission de Venise estime qu'au-delà de la prévention de l'interception ciblée des communications couvertes par le secret professionnel, la loi devrait mettre en place des

garanties renforçant la protection des communications de cette nature, même lorsqu'elles ont été interceptées accidentellement (...)

85. (...) la Commission de Venise recommande au législateur polonais d'envisager des règles plus strictes qui, tout en respectant les normes internationales en matière de droits de l'homme, décriraient les cas dans lesquels les communications couvertes par le secret professionnel pourraient être secrètement enregistrées puis utilisées comme preuve. »

D. Garanties procédurales

1. Durée de la surveillance et de la collecte de métadonnées

« 87. La loi autorise la mise en place d'une surveillance pour une période n'excédant pas trois mois (paragraphe 8 de l'article 19) ; une prolongation est possible, moyennant une décision de justice que le service compétent demande avec l'autorisation écrite du procureur, pour une période supplémentaire d'un maximum de trois mois si les motifs initiaux de mise en place de la surveillance sont encore valables. Dans les cas dûment justifiés (si des faits nouveaux nécessitent de prévenir ou de détecter une activité criminelle, ou d'en trouver les auteurs et d'obtenir des preuves), la surveillance peut être prolongée par une juridiction supérieure pour plusieurs périodes consécutives fixées par ladite juridiction, pour un total de 12 mois au maximum (paragraphe 9 de l'article 19). La surveillance ne doit pas durer plus de 18 mois au total.

88. La Commission de Venise constate que la durée maximale de surveillance que prévoit la loi est assez longue en soi. Mais le point le plus délicat est la possibilité de collecte de métadonnées pendant un temps indéterminé (article 20ca). La loi ne dit rien du volume de données historiques que peut consulter la police auprès des fournisseurs de services TIC, mais la durée de préservation de 12 mois constituera d'habitude une limite pratique. La loi ne précise pas non plus pendant combien de temps la police peut intercepter en direct les flux de métadonnées. Le principe de proportionnalité voudrait que ce soit spécifié. La Commission de Venise n'en reconnaît pas moins que la durée de conservation des données historiques et celle des périodes d'interception en direct et en continu des échanges de métadonnées (en particulier dans le cadre d'une surveillance stratégique) peuvent être relativement longues. »

2. Contrôle juridictionnel préalable et rétrospectif, dispositifs de traitement des plaintes et contrôle par un organe indépendant

(...)

a. Autorisation et contrôle des surveillances mises en place en vertu de l'article 19

i. Autorisation

« 91. L'article 19 impose qu'une surveillance soit préalablement autorisée par tribunal de district. Exceptionnellement, en cas de grande urgence, la police peut procéder sans cette autorisation à la surveillance, qu'elle devra interrompre si l'autorisation n'est pas obtenue dans les cinq jours, et toute l'information ainsi réunie devra alors être détruite (paragraphe 3).

92. (...) il serait souhaitable d'étendre l'impératif d'autorisation juridictionnelle préalable à la collecte de métadonnées se rapportant au contenu, très proche par sa nature de l'interception des communications relevant de l'article 19 (...).

93. (...) en Pologne, la dérogation [prévue au paragraphe 3 de l'article 19 pour les cas d'urgence] n'est pas justifiée par la gravité ou la nature de l'infraction, mais seulement par le risque de perte d'éléments de preuve. On ne voit par ailleurs pas clairement ce qui se passe si la police suspend l'interception « urgente » avant l'expiration du délai de cinq jours ; cette disposition, interprétée souplement, permettrait à la police de procéder sans contrôle juridictionnel à des interceptions de durée relativement brève. (...)

(...)

95. La seconde chose est l'absence de procédure contradictoire. La loi prévoit que le tribunal examine la demande de la police *ex parte*, sans la participation de la personne ciblée par la surveillance. (...) Sans débat contradictoire, le juge aura toutefois tendance à se montrer moins critique à l'égard de la position de la police. De plus, le risque de recours existe s'il rejette la demande, mais pas s'il l'accepte et ordonne surveillance. Dans ces conditions, l'autorisation juridictionnelle préalable de la surveillance pourrait bien devenir une pure formalité.

96. La loi fait bien d'impliquer un procureur dans le processus d'autorisation de la surveillance. Mais eu égard aux liens étroits entre le ministère public et la police dans le système polonais, cela ne paraît pas constituer une garantie procédurale suffisante.

97. Pour rendre le contrôle juridictionnel préalable plus efficace, il conviendrait de compléter le contrôle *ex parte* en faisant intervenir dans la procédure un « avocat de la vie privée » : un juriste indépendant, possédant les compétences techniques et les habilitations de sécurité nécessaires, et qui ne soit institutionnellement rattaché ni à la police ni au ministère public. Sa fonction serait de défendre les intérêts de la personne ciblée par la surveillance. »

ii. Contrôle rétrospectif

« 98. (...) Les informations obtenues par surveillance pourraient occasionnellement être utilisées comme éléments de preuve dans des poursuites pénales ; auquel cas l'examen de son affaire sur le fond donnerait à l'accusé, du moins en théorie, l'occasion de contester la légalité de sa surveillance. (...)

(...)

100. (...) en Pologne, les informations de « contrôle opérationnel » sont en général tenues secrètes. Il y a donc risque que la juridiction contrôlant l'ordre de surveillance dans la procédure sur le fond refuse de communiquer à la défense les informations relatives à l'autorisation de mise sur écoute. L'exclusion de ces informations dans l'examen contradictoire peut sensiblement désavantager la défense par rapport au ministère public, et donc être incompatible avec l'impératif de procès équitable.

101. (...) ce recours ne serait possible que dans une toute petite partie des affaires, uniquement lorsque l'existence de la surveillance a été mentionnée dans la procédure pénale. Dans la grande majorité des cas, la surveillance resterait « secrète ».

102. La loi pourrait habiliter dans ce cas la personne surveillée à déposer une plainte rétrospective. Mais pour se prévaloir de ce droit, il faut encore qu'elle ait connaissance de la

surveillance. (...) La Commission de Venise constate que la loi ne semble pas contenir d'exigence de notification de la personne ciblée, même après un certain temps.
103. La Commission de Venise comprend que la notification pourrait compromettre des méthodes confidentielles ou des opérations en cours. (...) Il n'en reste pas moins important que la loi impose aux autorités concernées une obligation générale de notification rétrospective, assortie de dérogations. Lorsque la personne apprend qu'elle a été surveillée, la procédure ex parte peut-être complétée par une procédure pleinement contradictoire ; la juridiction examine alors la légalité de la surveillance de *novo*. Il y aurait aussi la possibilité de créer un dispositif permanent non judiciaire auquel pourraient recourir les personnes inquiètes d'une éventuelle surveillance.

104. Il serait par ailleurs souhaitable d'autoriser explicitement le juge dont émane l'autorisation de surveillance à contrôler régulièrement les informations ainsi obtenues par la police. Cela lui permettrait de vérifier que la police n'outrepasse pas l'autorisation qu'il a initialement signée en vertu du paragraphe 1 de l'article 19, mais aussi de mieux comprendre l'utilité d'une mesure de ce type ainsi que l'ingérence qu'elle constitue. Il semble que la loi ne permette au juge de demander les informations obtenues par surveillance que dans le cas de la prolongation d'un mandat d'écoute ou, s'il s'agit de l'autorisation rétroactive d'une surveillance « urgente » mise en place sans autorisation préalable (paragraphes 3, 9 et 10 de l'article 19).

105. Une autre solution consisterait à mettre en place un système de contrôle rétrospectif des surveillances assuré par un organe indépendant agissant de sa propre initiative. La Commission de Venise constate que l'article 19 de la loi impose au ministère de l'Intérieur de soumettre chaque année au Parlement un rapport sur les surveillances menées par la police. Le ministère, prévoit l'article 19, ne doit toutefois donner qu'un aperçu général des activités de ce type, sans justifier la nécessité des opérations elles-mêmes. Ce dispositif ne saurait donc remplacer le contrôle des opérations de surveillances spécifiques par un organe indépendant qui connaisse bien les pratiques de surveillance et d'interception, et ne soit pas institutionnellement rattaché à la police ni trop proche du pouvoir exécutif et des services de répression ou de renseignement.

106. La Commission de Venise souligne que cet organe indépendant devrait être habilité à contrôler tous les aspects des opérations (dans le respect d'une discrétion opérationnelle raisonnable des services concernés), à consulter toutes les informations (même classifiées), et à engager toutes les actions récursoires appropriées en l'espèce.

107. La Commission de Venise souligne que l'autorisation de justice que prévoit actuellement l'article 19 pour la surveillance est au cœur du système garantissant le respect de la vie privée et d'autres droits fondamentaux des personnes ciblées. Mais elle devrait être complétée par d'autres garanties procédurales, notamment la possibilité de contrôle de la légalité et de la nécessité de la surveillance au cours de la procédure pénale qui s'ensuit, ou de plainte et de demande de contrôle juridictionnel si la surveillance n'a pas débouché sur des poursuites pénales. L'organisme de contrôle indépendant pourrait intervenir lorsqu'il n'y a pas eu de procédure pénale, et s'il n'est pas possible de faire jouer le dispositif de plainte du fait que la personne ciblée n'a pas été notifiée, pour des raisons valables, de la surveillance. L'organe de contrôle indépendant devrait être habilité à examiner les cas d'espèce de ce type et à soumettre

des recommandations et des rapports. Il n'est cependant pas nécessaire qu'il fasse office de cour d'appel à l'égard de la juridiction dont émanait l'autorisation de surveillance initiale.

108. La Commission de Venise a conscience qu'il faut du temps pour créer en Pologne un organe entièrement nouveau, et définir ses compétences par rapport à celles de la police, du ministère public et des tribunaux. Sachant que le pouvoir législatif polonais a dû agir rapidement, il n'est pas étonnant qu'un organe de ce type n'ait pas été créé pour décembre 2015. Mais la conception actuelle du système d'interception de métadonnées prévu à l'article 20c (voir paragraphes 110 et suivants) et la faiblesse du contrôle général des formes les plus intrusives de surveillance secrète (article 19) appelleraient la création d'un tel organe.

109. (...) l'autorisation de justice qu'exige l'article 19 est une garantie procédurale très utile ; mais elle ne suffit pas en soi à garantir la transparence de l'action de la police dans la surveillance secrète (ni des autres services de répression pouvant également s'y associer). Les autorités polonaises ont toute latitude pour concevoir un modèle qui garantisse le contrôle effectif des opérations de surveillance, pour autant qu'il s'appuie sur un organe indépendant (ou plusieurs) procédant à un contrôle effectif d'opérations spécifiques, et qu'il possède les instruments juridiques nécessaires pour détecter les abus et lutter contre eux. Les personnes placées sous surveillance devraient en être averties postérieurement de sorte qu'elles puissent être associées au contrôle ; si cela est impossible, d'autres mécanismes devraient permettre d'examiner l'affaire dans la perspective de la protection de la vie privée des personnes concernées par la surveillance, ou rendre possible un contrôle effectif de la légalité et du caractère raisonnable de ces mesures. »

b. Autorisation et contrôle de la collecte de métadonnées prévue à l'article 20ca

i. Autorisation

« 110. La loi n'assujettit pas à autorisation juridictionnelle la surveillance de métadonnées prévue à l'article 20c : dans la logique du droit polonais, la collecte de métadonnées est considérée comme constituant une ingérence moindre, et n'appelle donc pas des garanties procédurales aussi strictes que la surveillance « classique » de l'article 19. La Commission de Venise admet que, même s'il serait souhaitable que toute collecte de métadonnées soit préalablement autorisée par la justice, cette procédure peut parfois se révéler trop lourde pour la police. (...) Il suffirait de notifier postérieurement la juridiction (ou un organe de contrôle indépendant (...))

111. Les métadonnées se rapportant au contenu constituent la principale exception à cette règle : la Commission de Venise recommande aux autorités polonaises d'envisager de les intégrer dans le champ d'application de l'article 19 (si ce n'est pas déjà fait), en assortissant leur consultation de toutes les garanties procédurales (surtout l'autorisation préalable de justice). Il se serait également possible d'assujettir à autorisation préalable la collecte de métadonnées à grande échelle (si la cible est toute une zone géographique à un moment donné). Le contrôle rétrospectif d'opérations spécifiques devrait cependant constituer une garantie suffisante contre les abus pour la plupart des types de métadonnées. »

ii. Contrôle rétrospectif

« 112. L'article 20ca exige que la police soumette à une juridiction régionale compétente un rapport semestriel contenant une information générale sur la surveillance des métadonnées au cours de la période écoulée.

113. La Commission de Venise juge que cette obligation de soumettre des rapports ne suffit pas à assurer la transparence de l'action de la police en ce qui concerne la collecte de métadonnées. Ces documents ne contiennent que des informations synthétiques, mais rien de précis sur chaque opération. On voit mal les conclusions auxquelles peut arriver un juge à cette lecture. Certes, le magistrat peut demander de son propre chef à la police les informations qui ont justifié la communication de métadonnées à la police (paragraphe 3 de l'article 20ca) ; mais on ne sait pas très bien ce qu'il l'inciterait à mener une analyse individualisée de ce type. Dans le cas peu probable où il se montrerait proactif, étudierait les informations relatives à un cas d'espèce et détecterait des irrégularités, ses conclusions pourraient entraîner des poursuites pénales ou disciplinaires à l'encontre des membres de la police concernés.

114. Il convient alors de se demander si le contrôle rétrospectif devrait être confié à un tribunal ou à un organe indépendant. (...)

115. Une solution pourrait consister à associer plus étroitement les tribunaux au contrôle des opérations de surveillance de métadonnées, pour autant qu'ils disposent de suffisamment de ressources (temps, accès à des compétences techniques, compétences spéciales, etc.). Mais la question de l'interception des métadonnées est difficile à séparer d'autres aspects des enquêtes policières. Il pourrait être difficile pour les tribunaux ordinaires d'exercer en continu une sorte de fonction de contrôle de la police.

116. Il vaudrait mieux recourir à des organismes composés d'experts pour compléter ou remplacer le contrôle juridictionnel (...)

117. Quoi qu'il en soit, tout système de contrôle rétrospectif devrait s'appuyer sur un organe authentiquement indépendant et possédant les compétences et les pouvoirs nécessaires pour procéder convenablement au contrôle des surveillances de métadonnées. Comme pour la surveillance secrète (article 19), les autorités polonaises ont une très large latitude pour concevoir un système appuyé sur un organe indépendant qui obligerait la police à convaincre à l'extérieur de ses rangs un observateur indépendant de la nécessité de la mesure. La loi devrait charger l'organe de contrôle de procéder en permanence au contrôle proactif de toutes les opérations, et lui conférer les pouvoirs nécessaires à l'égard de la police et des procureurs. Elle pourrait aussi mettre en place une obligation qualifiée de notification et un dispositif de plainte (auprès d'un tribunal ou d'un organe de contrôle indépendant).

(...)

119. Pour simplifier la tâche de la police et décharger les tribunaux, le législateur polonais pourrait même exclure du champ d'application du contrôle rétrospectif la consultation par la police de données relatives à l'abonnement. S'il décide de le faire, ces opérations ne seront pas régulièrement examinées par les tribunaux (ou un autre organe indépendant), mais un système de journalisation devrait être mis en place, avec une forme quelconque de vérification rétrospective sur échantillons de la validité des opérations. En tout état de cause, en dehors des métadonnées les moins indiscrètes, toutes les opérations policières devraient pouvoir faire l'objet d'un contrôle rétrospectif effectif et complet. »

c. Accès direct aux métadonnées

« 120. Le paragraphe 3 de l'article 20c permet à la police d'accéder directement aux métadonnées sans participation du personnel des prestataires de services TIC dès lors que cela est prévu dans la convention passée par la police entre son haut commandement et le prestataire. Ce qui veut dire que la police aurait en permanence et directement accès aux métadonnées.

122. (...) les autorités ont assuré aux rapporteurs (...) que seuls certains agents désignés des forces de police avaient directement accès aux métadonnées chez les fournisseurs de services TIC110, et que la police enregistre toutes leurs connexions. Il s'agit de garanties minimales, qu'il convient de conserver. Mais en Pologne, les services de répression ont accès aux données sans même que les opérateurs de télécommunication le sachent, en quantités illimitées et à un coût très réduit (...), ce qui accroît considérablement les risques d'abus. Ces agents spécialement désignés, tout en étant des spécialistes, ne paraissent pas remplir une fonction d'élimination des demandes injustifiées (...), mais simplement de facilitation (c'est-à-dire de canal de communication). Le paragraphe 4 de l'article 20c n'en impose pas moins l'identification complète des agents des forces de police qui consultent des métadonnées, ce qui est une bonne chose.

123. La Commission de Venise constate que dans son état actuel, la loi ne confie pas le contrôle de la collecte de métadonnées à un organe indépendant chargé de vérifier que la police fait un usage raisonnable de ses pouvoirs, conformément aux bonnes pratiques d'enquête (...).

124. Il semble par ailleurs aux rapporteurs qu'il pourrait être difficile, en cas de consultation directe en temps réel, de séparer techniquement le contenu et les métadonnées. Il serait alors nécessaire d'insérer dans le système des modules garantissant que le contenu est clairement séparé des métadonnées, et que la police n'a accès qu'à ces dernières.

(...) »

VII. Conclusions

« (...)

133. La Commission de Venise recommande d'améliorer la loi en lui apportant les modifications essentielles suivantes (mais aussi les autres recommandations formulées au fil du texte du présent avis) :

– renforcer le principe de proportionnalité en étoffant les critères applicables à la surveillance secrète (article 19), ainsi qu'en ajoutant de nouveaux critères applicables à la collecte de métadonnées (article 20c), de sorte que la surveillance secrète et la collecte de métadonnées ne soient ordonnées que dans les cas les plus graves, surtout s'il s'agit d'une procédure d'urgence (article 19, paragraphe 3) ;

– interdire dans la loi la surveillance des communications *a priori* couvertes par le secret des communications entre l'avocat et son client, définir précisément les dérogations possibles à cette règle, et faire de même pour d'autres communications couvertes par le secret professionnel ;

– limiter la durée de la surveillance de métadonnées, exiger de la police qu'elle conserve des archives permettant le contrôle rétrospectif effectif des opérations de surveillance, surtout lorsqu'il s'agit d'« accès direct » ;

– compléter le système d'autorisation juridictionnelle préalable de la surveillance classique traitée à l'article 19 par d'autres garanties procédurales (un « avocat de la vie privée », un dispositif de plainte, un système de contrôle rétrospectif automatique de ces opérations par un organe indépendant, etc.)

– en ce qui concerne la collecte de métadonnées (article 20c), mettre en place un dispositif efficace de contrôle des opérations de ce type par un organe indépendant, doté des pouvoirs d'investigation et des compétences nécessaires, et habilité à engager les voies de recours appropriées.

(...) »

III. L'UNION EUROPÉENNE

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

93. Les articles 7, 8 et 11 de la Charte sont ainsi libellés :

Article 7 – Respect de la vie privée et familiale

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

Article 8 – Protection des données à caractère personnel

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

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

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

Article 11 – Liberté d'expression et d'information

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

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

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

1. *La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*

adoptée le 24 octobre 1995 (*la « directive sur la protection des données à caractère personnel »*)

94. La directive sur la protection des données à caractère personnel a régi pendant de nombreuses années la protection et le traitement des données à caractère personnel au sein de l'Union européenne. Elle ne s'appliquait toutefois pas aux activités des États membres relatives à la sécurité publique, à la défense et à la sûreté de l'État, celles-ci ne relevant pas du champ d'application du droit communautaire (article 3 § 2).

2. *La directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques adoptée le 12 juillet 2002 (la « directive vie privée et communications électroniques »)*

95. Dans ses considérants 2 et 11, la directive vie privée et communications électroniques énonce ce qui suit :

« 2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la charte des droits fondamentaux de l'Union européenne. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.

(...)

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

96. Les dispositions pertinentes de ladite directive se lisent ainsi :

Article premier – Champ d'application et objectif

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

ces données et des équipements et des services de communications électroniques dans la Communauté.

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

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

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

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

3. La directive 2006/24/CE sur la conservation de données

97. Avant l'arrêt du 8 avril 2014 de la CJUE qui l'a déclarée invalide (paragraphes 104-108 ci-dessous), la directive sur la conservation des données disposait notamment ce qui suit :

Article premier - Objet et champ d'application

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

2. La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne

s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques. »

Article 3 – Obligation de conservation de données

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

4. *Le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (*le « RGPD »*)

98. Le RGPD est entré en vigueur le 25 mai 2018, remplaçant la directive sur la protection des données. Il est d'application directe dans les États membres, et renferme des dispositions et des garanties relatives au traitement au sein de l'Union européenne des informations permettant d'identifier personnellement les individus qu'elles concernent. Il s'applique aux "personnes physiques" et ne couvre pas le traitement des données à caractère personnel concernant les personnes morales (considérant 14). En vertu de l'article 23 § 1, la législation des États membres peut restreindre la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34 « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir », entre autres, la sécurité nationale, la sécurité publique ou la prévention et la détection d'infractions pénales ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

99. Pareille législation doit notamment prévoir le droit des personnes concernées d'être informées, le cas échéant, de ladite limitation, à moins que cela ne risque de nuire à la finalité de celle-ci (article 23 § 2 h) du RGPD).

100. Toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du RGPD (article 77 § 1 du RGPD).

101. Toute personne concernée a également droit, dans les mêmes circonstances, à un recours juridictionnel effectif (article 79 § 1 du RGPD).

102. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD a le droit d'obtenir, du responsable du traitement ou du sous-traitant, réparation du préjudice subi (article 82 § 1 du RGPD). L'article 82 §§ 2 à 4 régit les modalités selon lesquelles cette réparation peut être demandée.

5. *La directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (la « directive « POLICE-JUSTICE »)*

103. La directive « POLICE-JUSTICE » régit le traitement, par les autorités compétentes, des données à caractère personnel des personnes physiques à des fins de « prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces » (articles 1 § 1 et 2 § 1). Aux termes de l'article 63 § 1, elle devait être transposée au plus tard en mai 2018. En Pologne, la loi du 14 décembre 2018 relative à la protection des données à caractère personnel traitées dans le cadre de la prévention et de la lutte contre la criminalité a procédé à la transposition requise.

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

1. *Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238)*

104. Par un arrêt du 8 avril 2014, la CJUE a déclaré invalide la directive 2006/24/CE sur la conservation des données, qui obligeait les fournisseurs de services de communications électroniques accessibles au public ou les réseaux publics de communications à conserver toutes les données relatives au trafic et les données de localisation pendant une durée de six mois à deux ans de manière à ce que ces données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne. Elle a jugé que l'obligation de conserver ces données constituait une ingérence dans le droit au respect de la vie privée et des communications et dans le droit à la protection des données à caractère personnel garantis respectivement par l'article 7 et par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

105. Elle a estimé également que l'accès des autorités nationales compétentes aux données constituait une ingérence supplémentaire dans ce droit fondamental, et que celle-ci était « particulièrement grave ». Elle a considéré que la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci étaient effectuées sans que l'abonné ou l'utilisateur inscrit en fussent informés était susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée faisait l'objet d'une surveillance constante. Elle a conclu que l'ingérence répondait à un objectif d'intérêt général, à savoir contribuer à la lutte contre la criminalité grave et le terrorisme et ainsi, en fin de compte, à la sécurité publique, mais qu'elle ne respectait pas le principe de proportionnalité.

106. En premier lieu, la directive couvrait de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves.

107. En deuxième lieu, la directive ne contenait pas les conditions matérielles et procédurales afférentes à l'accès des autorités nationales compétentes aux données et à l'utilisation ultérieure de celles-ci et elle ne subordonnait pas cet accès à un contrôle préalable par un tribunal où par une entité administrative indépendante dont la décision aurait visé à limiter l'accès aux données et leur utilisation à ce qui serait strictement nécessaire aux fins d'atteindre l'objectif poursuivi.

108. En troisième lieu, la directive imposait la conservation de toutes les données pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. Elle a considéré également que la directive ne prévoyait pas de garanties permettant d'assurer, par des mesures techniques et organisationnelles, une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites.

2. Tele2 Sverige (C-203/15 et C-698/15, EU:C:2016:970)

109. Dans cet arrêt rendu le 21 décembre 2016 sur renvoi préjudiciel de la cour administrative d'appel de Stockholm et de la cour d'appel d'Angleterre et du Pays de Galles, la CJUE a jugé qu'une législation nationale prévoyant la conservation générale de l'ensemble des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité était contraire à l'article 15 § 1 de la directive vie privée et communications électroniques. Elle a estimé que cette disposition s'opposait également à une législation permettant aux autorités d'accéder aux données conservées si cet accès (a) n'était pas limité à la seule finalité de lutte contre la criminalité grave, et (b) n'était pas soumis au contrôle préalable d'un tribunal ou d'une autorité indépendante. La CJUE a fondé ses conclusions, entre autres, sur la structure générale de la directive vie privée et communications électroniques, y compris le principe général de confidentialité des communications qu'elle énonçait, et sur l'exigence de stricte nécessité prévue par le droit de l'Union européenne à l'égard de toute limitation apportée à la protection des données à caractère personnel. Enfin, la CJUE a refusé de répondre à la question de savoir si la protection conférée par les articles 7 et 8 de la Charte, tels qu'interprétés par elle, était plus large que celle de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »). Elle a notamment relevé que le droit de l'Union européenne pouvait accorder une protection plus étendue que celle garantie par la Convention et que l'article 8 de la Charte concernait un droit (la protection des données à caractère personnel) qui n'avait pas d'équivalent dans la Convention.

3. Ministerio Fiscal (C-207/16, EU:C:2018:788)

110. Dans un arrêt du 2 octobre 2018 rendu à la suite d'un renvoi préjudiciel de la cour provinciale de Tarragone (Espagne), la CJUE a estimé que l'accès aux noms et adresses conservés donné aux autorités publiques en vue de l'identification des propriétaires de cartes SIM activées avec un téléphone portable volé constituait une ingérence qui, bien que non justifiée par la nécessité de lutter contre la criminalité « grave », ne revêtait pas une gravité suffisante pour contrevenir à l'article 15 § 1 de la directive vie privée et communications électroniques.

4. Privacy International (C 623/17, EU:C:2020:790) et La Quadrature du Net (C-511/18, C-512/18 et C 520/18; EU:C:2020:791)

111. Dans un arrêt rendu le 6 octobre 2020 (*La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791) sur renvoi préjudiciel du Conseil d'État français et de la Cour constitutionnelle belge, la CJUE a confirmé la conclusion énoncée dans l'affaire *Tele2 Sverige* précitée selon laquelle l'article 15 § 1 de la directive vie privée et communications électroniques s'opposait à une conservation générale aux fins de la lutte contre les formes graves de criminalité des données relatives au trafic et des données de localisation, et elle a estimé que cette disposition n'autorisait qu'une conservation ciblée de ces données, définie sur la base d'éléments objectifs et non discriminatoires. En revanche, l'article 15 § 1 ne s'opposait pas à la conservation générale (a) des adresses IP attribuées à la source d'une connexion Internet et (b) des données relatives à l'identité civile des utilisateurs des systèmes de communication. Elle a également considéré que la conservation générale des données relatives au trafic et à la localisation - pour une période (renouvelable) limitée au strict nécessaire - était permise si l'État concerné était confronté à une menace réelle et sérieuse, actuelle ou prévisible, pour sa sécurité nationale. Elle a toutefois précisé que la décision d'exiger la conservation générale des données en raison d'une telle menace devait faire l'objet d'un contrôle effectif, soit par un tribunal, soit par un organe administratif indépendant rendant une décision contraignante, et que ledit contrôle devait aussi porter sur le respect des conditions et des garanties requises en vertu de l'article 15 § 1.

112. Dans un autre arrêt du 6 octobre 2020 (*Privacy International*, C-623/17, EU:C:2020:790), la CJUE, statuant sur une question préjudicielle posée par l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni), a notamment jugé que l'article 15 § 1 de la directive vie privée et communications électroniques s'opposait à une législation permettant à une autorité d'exiger des fournisseurs de services de communications, aux fins de la sauvegarde de la sécurité nationale, qu'ils procèdent à une transmission générale des données relatives au trafic et des données de localisation aux agences de sécurité et de renseignement.

5. Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152)

113. Dans un arrêt du 2 mars 2021 rendu sur renvoi préjudiciel de la Cour suprême d'Estonie, la CJUE a rappelé que l'article 15 § 1 de la directive vie privée et communications électroniques n'autorisait l'accès, à des fins de lutte contre la criminalité, aux données relatives au trafic ou aux données de localisation conservées que lorsqu'étaient en cause des infractions graves ou des menaces graves pour la sécurité publique, et ce indépendamment de la durée de la période pour laquelle l'accès était demandé et de la quantité ou de la nature des données disponibles au cours de cette période. La CJUE a estimé en outre que l'examen des demandes d'accès ne pouvait pas être confié à un parquet, car ses fonctions en matière de direction de procédures préliminaires et de poursuites avaient une incidence sur son indépendance vis-à-vis des parties à la procédure pénale.

6. Commissioner of An Garda Síochána e.a (C-140/20, EU:C:2022:258)

114. Dans cet arrêt rendu le 5 avril 2022 sur renvoi préjudiciel de la Cour suprême d'Irlande, la CJUE a confirmé sa jurisprudence constante selon laquelle le droit de l'Union s'opposait à des mesures législatives nationales prévoyant, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques, aux fins de la lutte contre la criminalité grave. La CJUE a rejeté l'argumentation selon laquelle les autorités nationales compétentes devraient pouvoir accéder, aux fins de la lutte contre la criminalité grave, à ces données qui avaient été conservées de manière généralisée et indifférenciée pour faire face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Elle a observé que, selon ladite argumentation, l'accès pourrait être justifié par un objectif d'une importance moindre que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale, ce qui irait à l'encontre de la hiérarchie des objectifs d'intérêt général dans le cadre de laquelle doit s'apprécier la proportionnalité d'une mesure de conservation. Elle a estimé qu'autoriser un tel accès risquerait de priver de tout effet utile l'interdiction de procéder à une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave.

7. SpaceNet et Telekom Deutschland (C-793/19 et C-794/19, EU:C:2022:702)

115. Par cet arrêt rendu le 20 septembre 2022 sur renvoi préjudiciel de la Cour administrative fédérale allemande, la CJUE a confirmé sa jurisprudence (arrêts *La Quadrature du Net* et *Commissioner of An Garda Síochána*, paragraphes 111 et 114 ci-dessus) s'opposant à la conservation généralisée et indifférenciée, aux fins de la lutte contre la criminalité grave ou de la prévention des menaces graves contre la sécurité publique, des données relatives au trafic et des données de localisation, estimant que la législation nationale en cause n'était pas conforme au droit de l'Union européenne, malgré l'existence de garanties prévues par celle-ci et une durée de conservation plus courte (10 à 4 semaines) que dans les affaires précédentes. La CJUE a jugé en outre que la conservation de ces données et l'accès à celles-ci constituaient des ingérences distinctes dans les droits fondamentaux des personnes concernées, nécessitant une justification distincte, et que, par conséquent, la législation nationale assurant le plein respect des conditions résultant de la jurisprudence en matière d'accès aux donnés conservées ne saurait, par nature être susceptible ni de limiter ni même de remédier à l'ingérence grave dans les droits des personnes concernées qui résulterait de la conservation généralisée de ces données.

8. VD et SR (C-339/20 et C-397/20, EU:C:2022:703)

116. Dans cet arrêt rendu le 20 septembre 2022 sur renvoi préjudiciel de la Cour de cassation française, la CJUE a jugé que la directive « abus de marché » et le règlement relatif aux abus de marché, lus en combinaison avec la directive « vie privée et communications électroniques » et à la lumière de la Charte des droits fondamentaux de l'Union européenne, n'autorisaient pas une conservation généralisée et indifférenciée par les opérateurs de services de communications électroniques, pour une durée d'un an à partir du jour de leur enregistrement, des données relatives au trafic aux fins de la lutte contre les infractions d'abus de marché.

9. HYA et autres (Motivation des autorisations des écoutes téléphoniques) (C-349/21, EU :C:2023:102)

117. Dans cet arrêt rendu le 16 février 2023 sur renvoi préjudiciel du Tribunal pénal spécialisé bulgare, la CJUE a conclu qu'une décision autorisant une mise sur écoute téléphonique pouvait ne pas contenir de motifs individualisés. Elle a en effet considéré que pareille décision n'emportait pas violation de l'obligation de motivation dès lors qu'elle se fondait sur une demande détaillée et circonstanciée de l'autorité pénale compétente et que les motifs de l'autorisation pouvaient être déduits aisément et sans ambiguïté d'une lecture croisée de la demande et de l'autorisation.

IV. ÉLÉMENTS DE DROIT COMPARÉ

118. La Cour a procédé à une étude comparative du droit et de la pratique internes de trente-cinq États parties à la Convention[7] relativement à la question des garanties de protection existant à l'égard des personnes privées vis-à-vis des organismes qui appliquent la surveillance secrète.

119. Il ressort des contributions reçues des États sur lesquels porte l'étude que dans la plupart d'entre eux (trente-et-un États) la surveillance exercée dans un but de lutte contre la criminalité est soumise à un contrôle préalable d'un organe judiciaire[8]. Il apparaît en outre que sur l'ensemble des concernés, quinze ont instauré, en sus du contrôle *a priori*, un contrôle *a posteriori* de la surveillance. Celui-ci est assuré par les tribunaux (neuf États)[9], par des organes relevant du pouvoir exécutif (un État)[10], par des organes parlementaires (deux États)[11] ou par des organismes hybrides (trois États)[12]. Par ailleurs, certains des États étudiés ont introduit des dispositions relatives aux situations d'urgence dans lesquelles la surveillance peut être autorisée par un procureur mais doit être interrompue si l'autorisation judiciaire n'est pas obtenue à bref délai. Quant à la surveillance exercée par les services spéciaux dans un but de prévention de certaines infractions le plus graves ou celui de protection de sécurité et/ou d'intérêts essentiels de l'État, les législations respectives de dix-huit des États concernés[13] font dépendre la mise en place de la surveillance en question d'une autorisation préalable émanant d'un organe judiciaire ou relevant du pouvoir exécutif (trois États)[14] ou encore d'un organe à caractère mixte ou hybride (six États)[15]. En revanche, seuls cinq États[16] prévoient un contrôle judiciaire *a posteriori* des mesures de surveillance de ce type, que ce soit à titre exclusif ou en complément d'autres mécanismes de contrôle. Ainsi en France, en particulier, le contrôle en question est effectué par le Conseil d'État, qui, dès lors qu'il conclut au caractère irrégulier de la mesure de surveillance dont il a à connaître, annule l'autorisation y afférente, ordonne la destruction des éléments collectés dans le cadre de ladite surveillance et informe la personne visée par la mesure en question de sa qualité de victime de surveillance irrégulière. De même, au Royaume-Uni, l'Investigatory Power Tribunal statue sur les plaintes d'individus dénonçant une surveillance mise en place à leur égard. Enfin, dans trois États, le contrôle *a posteriori* des mesures de surveillance est confié à des organismes relevant du pouvoir exécutif. Dans treize des États concernés[17] un contrôle *a posteriori* de la surveillance en question est assuré par les parlements nationaux, des commissions ou des comités parlementaires et dans huit autres États[18] ledit contrôle est confié aux organismes à caractère hybride. Enfin, dans trois des États concernés[19] les services de l'État en question font l'objet de la supervision par des organes relevant du pouvoir exécutif.

120. Vingt-et-un des États inclus dans l'étude imposent aux organismes ayant recours à la surveillance dans un but de lutte contre la criminalité une obligation de notifier celle-ci, après sa réalisation, à la personne visée. Huit États[20] ont indiqué que leurs législations respectives prévoyaient une telle obligation relativement à la surveillance effectuée dans un but de protection de sécurité nationale. De plus, six autres États n'ont instauré aucune obligation en la matière. Dans certains des huit États susvisés, un organisme compétent peut s'opposer à ladite notification en cas de danger pour la sécurité nationale ou pour la vie ou la santé de personnes privées, ou de risque d'entrave à la bonne marche d'une enquête pénale. Dans la plupart des trente-cinq États concernés par l'étude, l'individu qui a fait l'objet d'une surveillance peut, selon le cas, soit l'attaquer devant un tribunal ordinaire en formant un recours contre la décision l'ayant autorisée, soit inviter le tribunal compétent à en contrôler la légalité, et/ou contester la régularité des éléments de preuve issus de la surveillance en question. De plus, neuf des États concernés[21] ont instauré de recours similaires en matière de surveillance secrète qui est réalisée dans un but de protection de sécurité nationale. En cas de préjudice occasionné à une personne par une mesure de surveillance appliquée à son insu, l'individu en question peut, selon l'État concerné, soit en demander réparation dans le cadre d'une action en dommages et intérêts, soit réclamer que des poursuites soient engagées contre les agents des services de l'État compétents qu'il estime responsables des abus. De plus, onze États ont instauré des recours spécifiques en la matière, soit en lieu et place de recours judiciaires, soit en complément de ceux-ci. L'examen des recours formés dans ce cadre est confié, selon le cas, à des organismes hybrides analogues à ceux chargés de la supervision de la surveillance (sept États)[22] ou à des instances parlementaires et/ou celles relavant du pouvoir exécutif (quatre États)[23].

121. En sus desdits recours, les États concernés ont introduit dans leurs législations respectives des garanties complémentaires visant à protéger les personnes soumises à une surveillance contre d'éventuels abus de la part des organismes qui l'appliquent. Les garanties en question englobent, entre autres, un catalogue énumérant limitativement les infractions pour lesquelles une surveillance peut être autorisée, une obligation de délivrer l'autorisation requise sous forme écrite et/ou de la motiver, ou de la soumettre au respect de conditions matérielles (nécessité, proportionnalité, subsidiarité) concernant la surveillance, une limitation des possibilités de prolongation de la durée de la mesure, une obligation pour les autorités compétentes de procéder, à la clôture de la procédure pénale pour laquelle des éléments de preuve ont été collectés ou à l'expiration d'un délai courant à compter de la réalisation de la surveillance, à la destruction desdits éléments de preuve obtenus dans le cadre de la mesure, la participation obligatoire à la procédure d'autorisation d'une mesure de surveillance du défenseur des intérêts de la personne visée par celle-ci, ainsi enfin qu'une réglementation approfondie des questions relatives à l'accès, à la transmission et à l'utilisation des informations collectées dans le cadre de la surveillance et, tout particulièrement, de celles qui sont couvertes par le secret professionnel. En outre, dans huit États, les autorités effectuant la surveillance sont en plus soumises à la supervision des organismes de protection des données à caractère personnel, lesquels disposent d'une expertise technique poussée en matière de surveillance.

122. Sur l'ensemble des États inclus dans l'étude, vingt[24] ont mis en place une réglementation en matière de conservation et de traitement de données de communication par

leurs services de police et de renseignement respectifs. Dans seize États[25], ce type de surveillance est soumis à une procédure d'autorisation analogue à celle applicable au contrôle opérationnel, et dans trois États[26], elle ne fait apparemment l'objet d'aucune forme de contrôle judiciaire. Enfin, dix États n'ont pas communiqué d'information à la Cour quant à la pratique de leurs services compétents respectifs relativement à l'application de ce type de surveillance.

123. Dix-neuf États[27] ont introduit dans leur législation des dispositions spécifiques relativement à la surveillance « stratégique »[28], et seize États ne disposent d'aucune règlementation en la matière. Dans onze des dix-neuf États susvisés[29], la mesure de surveillance en question fait objet d'un contrôle *a priori* assuré par des organismes judiciaires, et dans deux États[30] ledit contrôle est confié à des organismes relevant du pouvoir exécutif. La majorité des États concernés soumettent ce type surveillance à un contrôle *a posteriori*, qui est exercé, selon le cas, par des organes parlementaires (sept États)[31], judiciaires (quatre États)[32], hybrides (six États)[33] ou relevant du pouvoir exécutif (deux États)[34]. Dans cinq États, les mesures de surveillance stratégique peuvent faire l'objet d'une contestation dans le cadre d'une procédure judiciaire[35], et onze États prévoient, en sus de pareille procédure judiciaire ou en lieu et place de celle-ci, une procédure spéciale par laquelle la surveillance peut être attaquée, selon le cas, devant un organisme hybride (sept États)[36] ou devant une instance parlementaire ou relevant du pouvoir exécutif (quatre États)[37]. Enfin, cinq États ont instauré une obligation de notification de ce type de surveillance aux personnes visées par celles-ci.

EN DROIT

I. JONCTION DES REQUÊTES

124. Eu égard à la similarité de l'objet des requêtes, la Cour juge opportun de les examiner ensemble dans un arrêt unique.

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

125. Invoquant l'article 8 de la Convention, seul et combiné avec l'article 13, les requérants se plaignent, tout d'abord, des systèmes de surveillance secrète et de conservation et de traitement de données de communication mis en place en application de la loi du 15 janvier 2016 et de la loi anti-terrorisme, estimant qu'ils portent atteinte à leur droit au respect de leur vie privée. Ils soutiennent ensuite qu'ils ne disposent d'aucun recours effectif pour faire établir s'ils ont eux-mêmes fait l'objet d'une surveillance secrète et, le cas échéant, faire contrôler la légalité de celle-ci.

126. Le Gouvernement conteste ces allégations.

127. En vertu du principe *jura novit curia*, la Cour n'est pas tenue par les moyens de droit avancés par les requérants en vertu de la Convention et de ses Protocoles, et elle peut décider de la qualification juridique à donner aux faits d'un grief en examinant celui-ci sur le terrain d'articles ou de dispositions de la Convention autres que ceux invoqués par les requérants (*Radomilja et autres v. Croatie* [GC], nos 37685/10 et 22768/12, § 126, 20 mars 2018). En l'espèce, elle examinera les faits de la présente espèce à la lumière des dispositions pertinentes de l'article 8 de la Convention, lesquelles sont ainsi libellées :

Article 8

« 1. Toute personne a droit au respect de sa vie privée (...)

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

A. Sur la recevabilité

Sur les exceptions préliminaires soulevées par le Gouvernement relativement à une incompatibilité ratione personae *de la requête avec les dispositions de la Convention et à un non-épuisement des voies de recours internes*

128. Le Gouvernement soutient, d'une part, que les requérants ne peuvent se prétendre victimes d'une violation de leur droit au respect de leur vie privée et, d'autre part, qu'ils n'ont pas épuisé les voies de recours internes. Les requérants quant à eux contestent les arguments avancés par le Gouvernement à l'appui de ces exceptions.

129. La Cour considère que les exceptions formulées par le Gouvernement sont étroitement liées à la substance des griefs des requérants et qu'il y a lieu par conséquent de les joindre au fond (voir, *mutatis mutandis, Roman Zakharov c. Russie* [GC], no 47143/06, § 150, 4 décembre 2015).

130. Constatant par ailleurs que les griefs soulevés sous l'angle de l'article 8 ne sont pas manifestement mal fondés ni irrecevables pour un autre motif visé à l'article 35 de la Convention, la Cour les déclare recevables.

B. Sur le fond

1. Sur la qualité de victime des requérants et l'existence d'une « ingérence »

a) Arguments des parties

i. Le Gouvernement

131. Le Gouvernement estime que les requérants ne peuvent se prétendre victimes d'une violation de l'article 8 de la Convention et que leurs requêtes respectives sont de type *actio popularis*. Selon lui, la qualité de victime des requérants dépend des conditions qui ont été énoncées dans l'affaire *Roman Zakharov* (arrêt précité), lesquelles ne seraient pas réunies en l'espèce. À cet égard, il argue que les intéressés n'ont fourni aucune preuve à l'appui de leurs allégations relatives à la mise en place d'une surveillance les concernant et que celles-ci sont par conséquent spéculatives. Ainsi, ils se borneraient à mettre en cause la conformité de la législation en question à la Convention. Le Gouvernement soutient en outre que les requérants, qui sont de nationalité polonaise, ne peuvent se plaindre de la surveillance prévue à l'article 9 de la loi anti-terrorisme dès lors que cette disposition ne s'applique qu'aux seuls ressortissants étrangers.

132. Il considère par ailleurs que les requérants avaient à leur disposition des recours internes qu'il leur reproche de ne pas avoir exercés. Il expose tout d'abord qu'ils auraient pu, sur le

fondement de l'article 2 § 1 de la loi sur l'accès à l'information publique, inviter les autorités publiques compétentes à leur communiquer les informations prétendument collectées à leur insu dans le cadre d'une mesure de surveillance secrète, lesquelles informations sont, selon lui, qualifiées de « publiques » par la Cour administrative suprême dans sa jurisprudence pertinente. Il ajoute qu'en cas de refus de la part desdites autorités de faire droit à pareille demande, les requérants auraient pu attaquer les décisions de rejet devant les tribunaux administratifs de deux degrés. À cet égard, il précise que les requérants Wojciech Klicki et Katarzyna Szymielewicz, qui ont formé une telle demande auprès du chef de l'ABW, n'ont pas utilisé le recours dont ils disposaient pour contester la décision de celui-ci devant les juridictions administratives. Il soutient en outre que si les requérants estimaient que les dispositions de l'article 5 § 1 de la loi sur l'accès à l'information publique, pour autant qu'elles ne leur permettaient pas d'accéder aux informations prétendument obtenues à leur insu au moyen d'une surveillance secrète, étaient attentatoires à leur droit au respect de leur vie privée, ils auraient pu - dans le cas où ils auraient exercé en vain les recours susmentionnés devant les tribunaux administratifs – s'en plaindre devant la Cour constitutionnelle en arguant qu'elles étaient contraires aux articles 47, 49 et 51 § 3 de la Constitution. Selon le Gouvernement, si la Cour constitutionnelle avait statué en faveur des intéressés, les autorités nationales concernées se seraient trouvées dans l'obligation de modifier la législation pertinente, et les requérants auraient alors pu engager une action en dommages et intérêts contre l'État sur le fondement de l'article 417[1] du CC. Par ailleurs, le Gouvernement est d'avis que le recours prévu à l'article 227 du CPA revêt un caractère informel et non contraignant vis-à-vis des autorités, et que les requérants ont par conséquent exercé un recours qui était ineffectif et inadéquat en l'espèce. Sur ce point, s'il admet que le recours en question était de nature à permettre aux intéressés d'attirer l'attention des autorités sur d'éventuelles irrégularités, il explique qu'il ne pouvait en aucun cas donner lieu à une quelconque solution juridictionnelle quant au litige des intéressés, et conclut qu'il n'était qu'un subterfuge pour saisir la Cour. Enfin, il reproche aux requérants de ne pas avoir soulevé devant les autorités nationales, pour ce qui est du premier requérant, les griefs tirés d'une violation des droits de la défense de ses clients et du droit à un procès équitable et, pour ce qui concerne l'ensemble des requérants, les griefs tenant à la mise en place, à leur insu, d'une surveillance à leur endroit en application de la loi anti-terrorisme.

ii. Les requérants

133. Les requérants rejettent les arguments du Gouvernement.

134. Ils considèrent qu'ils peuvent bel et bien se prétendre victimes d'une violation de l'article 8 de la Convention, à la fois du fait de la simple existence d'une législation sur la surveillance secrète et en raison de leurs situations personnelles respectives. Ils arguent tout d'abord que le champ d'application de la législation incriminée est large, expliquant que celle-ci est applicable à toute personne placée sous la juridiction de l'État polonais sans aucune exception relative aux journalistes, aux avocats de la défense ou aux militants des droits de l'homme. Ils ajoutent que la surveillance prévue à l'article 9 de la loi anti-terrorisme concerne également les individus avec lesquels l'étranger qui en fait l'objet est en contact, même si formellement ils sont hors du champ d'application de la disposition en question. Ils soutiennent ensuite qu'ils sont eux-mêmes exposés à un risque accru de se voir appliquer pareille surveillance, eu égard à leurs situations personnelles et professionnelles

respectives. Le requérant Mikołaj Pietrzak allègue ainsi qu'il est intervenu, en sa qualité d'avocat, dans d'importantes affaires pénales, dont certaines étaient politiquement sensibles, ainsi que dans des dossiers relevant du contentieux des étrangers, à l'égard de clients qui, pour certains d'entre eux, faisaient l'objet d'une surveillance secrète. Quant aux autres requérants, ils précisent que les ONG pour lesquels ils travaillent dispensent un soutien juridique aux étrangers, parmi lesquels des réfugiés, et qu'elles œuvrent, entre autres, pour la protection des individus face aux services de l'État qui effectuent des surveillances au moyen des nouvelles technologies. Ils estiment que les données sensibles dont ils sont en possession du fait de leurs activités professionnelles respectives font d'eux des cibles par excellence des autorités chargées de la surveillance, et qu'il en va d'autant plus ainsi en l'absence de mécanisme de protection efficace contre les éventuels abus commis par celles-ci. Le requérant Mikołaj Pietrzak expose en particulier que les moyens techniques dont disposent les services de l'État concernés sont, à n'en pas douter, plus performants que les mesures qu'il dit avoir prises pour garantir la confidentialité de ses échanges professionnelles avec ses clients, et que celles-ci ne sont par conséquent nullement un gage de sécurité desdits échanges en l'espèce. En outre, il ressort selon lui d'éléments statistiques pertinents détenus par les autorités du barreau de Varsovie qu'au cours de la période allant de juin 2016 à septembre 2022, les avocats membres de ce barreau ont signalé auxdites autorités environ trois cent vingt-cinq tentatives d'atteintes à la confidentialité de leurs échanges professionnelles.

135. Les requérants soutiennent par ailleurs, d'une part, que le droit polonais n'offre aucun recours qui leur aurait permis, le cas échéant, de faire établir l'existence d'une mesure de surveillance les concernant et d'en faire contrôler la légalité et, d'autre part, que la législation applicable n'impose aux services de l'État compétents en la matière aucune obligation de notification des mesures de surveillance aux personnes visées, même en cas de demande expresse en ce sens de la part de celles-ci, ce qui, selon eux, rend impossible toute contestation de la légalité de pareille mesure par les personnes surveillées. Ils estiment que les recours invoqués par le Gouvernement sont dépourvus de tout effet utile, arguant qu'il n'a fourni aucun exemple de décision interne susceptible de prouver le contraire. Ils font également observer qu'en l'espèce, deux d'entre eux ont exercé, sans succès, le premier des recours indiqués par l'État défendeur. De leur avis, il découle des dispositions législatives sur le fondement desquelles le chef de l'ABW a rejeté leurs demandes que les informations collectées au moyen d'une surveillance secrète sont confidentielles, et qu'il était par conséquent contraint d'en refuser l'accès à quiconque en aurait fait la demande. Ils ajoutent que ces considérations s'appliquent à l'ensemble des services de police et de renseignement ayant recours à la surveillance. Quant à la contestation de la décision du chef de l'ABW devant le tribunal administratif, ils considèrent qu'elle était vouée à l'échec eu égard à la jurisprudence constante de la Cour administrative suprême – celle-là même à laquelle le Gouvernement se réfère dans ses observations –, expliquant que ladite juridiction indique non seulement que les informations collectées par les services de police et de renseignement au moyen d'une surveillance secrète sont « publiques », mais également qu'en application de l'article 5 de la loi sur la protection de l'accès à l'information publique, l'accès à ces informations est soumis à des restrictions, parmi lesquelles celles qui sont énoncées dans la loi sur la protection des données classées. Ainsi, l'approche jurisprudentielle de la Cour administrative suprême en la matière

pourrait être résumée comme suit : « les restrictions à l'accès aux informations publiques relatives au fonctionnement des services secrets, pour autant qu'elles résultent de la nécessité d'assurer la protection des informations confidentielles, sont justifiées ».

136. Pour ce qui est de la plainte devant la Cour constitutionnelle que le Gouvernement les estimait tenus de former dans le cas où les recours qu'ils auraient dû, selon lui, introduire devant les autorités et tribunaux administratifs n'auraient pas prospéré, les requérants soutiennent, outre que lesdits recours étaient en tout état de cause inefficaces, qu'elle ne saurait être considérée comme « un recours à épuiser », au sens de la jurisprudence de la Cour, et ce pour plusieurs raisons. Premièrement, ils exposent que pour être recevable, une plainte constitutionnelle doit mettre en cause la ou les dispositions législatives sur lesquelles le tribunal ou l'autorité publique compétents a fondé la décision contestée devant la Cour constitutionnelle. Ils expliquent qu'en l'espèce, il ressort des décisions rendues par le chef de l'ABW concernant le requérant Wojciech Klicki et la requérante Katarzyna Szymielewicz que cette autorité a fait application de toute une série de dispositions législatives, et non pas seulement de l'article 5 de la loi sur l'accès à l'information publique. Ils considèrent ainsi que, contrairement à ce que le Gouvernement avance dans ses observations, la contestation du seul article 5 par eux devant la Cour constitutionnelle aurait été insuffisante au regard des conditions rigoureuses de recevabilité que la plainte constitutionnelle aurait dû satisfaire. Deuxièmement, ils arguent que pareille plainte constitutionnelle aurait donné lieu au contrôle par la Cour constitutionnelle de la seule réglementation du fonctionnement de l'ABW, et non pas de l'ensemble des dispositions pertinentes, et que par conséquent conclure qu'ils auraient dû engager plusieurs procédures administratives ainsi qu'un recours devant la Cour constitutionnelle pour satisfaire à l'exigence de l'épuisement des voies de recours internes devant la Cour de Strasbourg serait excessif. Troisièmement, ils font observer qu'un arrêt rendu en leur faveur par la Cour constitutionnelle n'aurait pas entraîné automatiquement l'invalidation des décisions de rejet émanant du chef de l'ABW et des tribunaux administratifs, mais qu'il aurait seulement constitué, sous certaines conditions, une base à la réouverture de la procédure afférente, procédure dont l'objet aurait été par ailleurs limité, selon eux, à la seule question de l'accès aux informations confidentielles collectées par l'ABW. Ils ajoutent qu'une plainte constitutionnelle ne leur aurait pas davantage permis de faire contrôler la légalité d'une éventuelle surveillance mise en place à leur égard, ni d'obtenir réparation dans le cas où celle-ci aurait été illicite. Quatrièmement, ils estiment que la plainte constitutionnelle ne satisfait pas aux exigences du recours effectif en raison des controverses dont la Cour constitutionnelle est actuellement l'objet, lesquelles ont donné lieu, indiquent-ils, à l'arrêt *Xero Flor (Xero Flor w Polsce sp. z o.o. c. Pologne*, no 4907/18, 7 mai 2021) de la Cour européenne des droits de l'homme. Cinquièmement, se référant à la jurisprudence de la Cour constitutionnelle (paragraphes 70–73 ci-dessus), ils arguent que la haute juridiction a déjà examiné des griefs analogues à ceux sur lesquels porte la présente espèce, qu'à cette occasion elle a conclu à l'inconstitutionnalité des dispositions litigieuses, et qu'en conséquence l'exercice par eux d'un recours devant la Cour constitutionnelle aurait été inutile. Ils soutiennent en outre que la législation qui était censée mettre la réglementation incriminée en conformité avec les principes dégagés par la Cour constitutionnelle a en réalité aggravé la situation à cet égard, et qu'en tout état de cause l'actuelle Cour constitutionnelle a déclaré (paragraphe 76 ci-dessous) qu'aucun contrôle juridictionnel ne s'imposait concernant les décisions autorisant des mesures de

surveillance. Sixièmement, rappelant qu'ils ont formé un recours en application de l'article 227 du CPA, ils allèguent, d'une part, que ledit recours leur a permis de dénoncer l'ensemble des opérations de surveillance conduites en secret par les services de l'État concernés et, d'autre part, qu'il a donné l'occasion à ceux-ci de répondre à l'ensemble de leurs griefs concernant les opérations en question. Ils considèrent par ailleurs qu'une action en dommages et intérêts dirigée contre l'État sur le fondement de l'article 417[1] du CC aurait été inefficace, expliquant que pareille action requérait que le caractère irrégulier de la surveillance les concernant fût démontré, et que cette exigence ne pouvait être satisfaite en l'absence d'une quelconque notification à eux de la surveillance en question. Enfin, en réponse à l'argument du Gouvernement selon lequel ils n'auraient pas soulevé devant les autorités nationales certains de leurs griefs relatifs à la surveillance réalisée en application de l'article 9 de la loi anti-terrorisme, ils arguent que dans leurs recours respectifs, ils mettaient en cause la possibilité pour les services de l'État de recourir à la surveillance secrète dans son ensemble, et que par conséquent leurs griefs portaient également sur la surveillance effectuée en application de la dispositions en question.

137. Les requérants concluent que la qualité insuffisante de la législation applicable, combinée avec l'absence d'un mécanisme de contrôle de la surveillance indépendant et l'absence dans leur chef d'un recours effectif en la matière, est de nature à leur faire craindre à juste titre que leurs communications sont surveillées.

b) Appréciation de la Cour

i. Principes généraux

138. La Cour observe qu'en l'espèce, les requérants allèguent une ingérence dans l'exercice de leur droit protégé par l'article 8 de la Convention, laquelle ingérence découlerait non pas de mesures spécifiques de surveillance qui leur auraient été appliquées, mais de la simple existence d'une législation autorisant la surveillance secrète de leurs communications ainsi que d'un risque de faire eux-mêmes l'objet de telles mesures.

139. La Cour rappelle que les principes généraux quant à la question de savoir si les requérants peuvent se prétendre « victimes » de la violation de l'article 8 entraînée par la simple existence de la législation ou de la pratique nationales autorisant la surveillance secrète ont été énoncés dans l'arrêt *Roman Zakharov* (*Roman Zakharov*, précité, § 171) et réitérés ultérieurement dans les arrêts *Centrum för rättvisa c. Suède* [GC], no 35252/08, § 167, 25 mai 2021 et *Ekimdzhiev et autres c. Bulgarie*, no 70078/12, § 262, 11 janvier 2022.

ii. Application à la présente affaire

140. En l'espèce, la Cour relève que les requérants dénoncent les dispositions relatives à la surveillance secrète, telles qu'elles sont mises en application par divers services de police et de renseignement nationaux. Elle note, d'une part, que le régime juridique de surveillance est constitué de plusieurs lois règlementant les activités respectives desdits services de l'État et, d'autre part, que l'ensemble des textes pertinents prévoient un modèle de surveillance quasi analogue. Elle observe de plus qu'en la matière, la loi sur la police constitue l'exemple *mutatis mutandis* pour les autres organismes.

141. La Cour constate que, s'agissant de la surveillance secrète, la législation nationale instaure deux régimes juridiques différents, à savoir un régime relatif au contrôle opérationnel, et un autre portant sur la conservation et le traitement des données de communication. Elle note que les deux types de surveillance en question font l'objet d'une règlementation prévue, respectivement, à l'article 19 et à l'article 20 c de la loi sur la police. Elle observe, de plus, que la première desdites dispositions fait relever du contrôle opérationnel des mesures qui permettent aux autorités de connaître le contenu de communications obtenues par des moyens tels que, notamment, les écoutes, l'enregistrement de conversations téléphoniques, de mails ou de messages déposés sur répondeur, l'interception de la correspondance postale ou encore l'enregistrement sur le vif de conversation à l'aide de dispositifs appropriés (paragraphe 31 ci-dessous). Il est évident, aux yeux de la Cour, que pareilles mesures de surveillance impliquent une intrusion dans la sphère privée des particuliers ciblés par les agences de l'État qui la diligentent. Quant aux données de communication, la Cour relève qu'elles englobent des informations relatives notamment aux appels téléphoniques effectués ou reçus, aux numéros composés, à la durée des appels, à la localisation géographique des appareils mobiles, aux sites Internet consultés, aux connexions à des sites et aux adresses mails (paragraphe 46 ci-dessous). À cet égard, elle rappelle avoir dit que « si le contenu d'une communication, crypté ou non, peut ne rien révéler d'utile sur son expéditeur ou son destinataire, les données de communications associées, en revanche, peuvent révéler un grand nombre d'informations personnelles (...) [et que] toute intrusion occasionnée par l'acquisition de données de communication associées est démultipliée par l'interception en masse, car ces données peuvent [alors] faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée (...) » (*Big Brother Watch et autres c. Royaume-Uni* [GC], nos 58170/13 et 2 autres, § 342, 25 mai 2021).

142. La Cour note que l'article 19 § 1 de la loi sur la police permet aux fonctionnaires de la police nationale de diligenter en secret les mesures opérationnelles d'enquête en vue de la prévention ou de la découverte d'infractions, de la découverte des auteurs de ces infractions et de la collecte et de l'enregistrement des éléments de preuve. Elle constate que le catalogue d'infractions pour lesquelles les mesures de surveillance en question peuvent être appliquées par les agents de l'État concernés est libellé en des termes larges, et relève, en outre, que plusieurs services spéciaux de l'État peuvent mettre en place pareilles mesures de surveillance à des fins utiles à la réalisation de leurs missions statutaires respectives. Renvoyant aux conclusions de la Cour constitutionnelle dans l'arrêt K 23/11 (précité), la Cour retient également que le champ d'application *ratione personae* du contrôle opérationnel est large. De plus, se reportant à l'avis de la Commission de Venise susmentionné (paragraphe 92 ci-dessus), elle observe que cette instance a considéré, d'une part, que « l'objet de surveillance n'était pas clairement précisé dans la loi sur la police » et, d'autre part, que « n'importe quelle personne ou groupe [pouvait vraisemblablement être visé] pour autant que l'on pouvait probablement obtenir ainsi des informations qui permettraient d'atteindre les but définis à l'article 19 [de la loi sur la police] pour la surveillance et à l'article 20c [de la même loi] pour la collecte de métadonnées ». Pour ce qui est, en particulier, de la surveillance de ce dernier type, la Cour a égard au fait que la législation y relative ne contient aucune précision quant aux catégories de personnes dont les communications sont susceptibles d'être surveillées. La Cour est d'avis que la législation litigieuse, ainsi qu'il ressort des constats de l'avis de la Commission de Venise exposés ci-dessus, a instauré un système de surveillance dans le cadre duquel pratiquement tout usager des services de

télécommunication et d'Internet peut voir intercepter ses communications, sans jamais être informé de la surveillance le concernant. Quant aux dispositions de la loi anti-terrorisme, la Cour relève, à l'instar des requérants que, même si le champ d'application *ratione personae* de loi en question est limité aux seuls ressortissants étrangers soupçonnés d'activités terroristes, toute personne qui a été en contact avec ces derniers peut voir ses communications surveillées indirectement, nonobstant qu'elle ait été elle-même ou non placée sous surveillance (*mutatis mutandis Ekhimdzhiev et autres*, précité, § 263).

143. La Cour estime par ailleurs que, pour les motifs exposés ci-dessous aux paragraphes 241-245, le droit polonais n'offre pas de recours effectifs à une personne qui pense avoir fait l'objet d'une surveillance secrète (voir, *mutatis mutandis, Roman Zakharov*, précité, § 176).

144. Elle considère par conséquent qu'en l'espèce, les requérants n'ont pas à établir qu'ils sont exposés au risque de faire l'objet d'une surveillance secrète en raison de leurs situations personnelles respectives (pour un raisonnement analogue, voir, *idem*, § 177 et *Ekimdzhiev et autres*, précité, § 276).

145. Eu égard au caractère secret et au large champ d'application des mesures de surveillance prévues par la législation contestée par les requérants ainsi qu'à l'absence de recours internes effectifs au moyen desquels les personnes qui se croient surveillées pourraient contester les mesures de surveillance supposément diligentées à leur endroit, la Cour estime justifié l'examen *in abstracto* de la législation litigieuse (*idem*, § 277).

146. Dès lors, elle considère que les requérants peuvent se prétendre victimes d'une violation de la Convention bien qu'ils ne puissent alléguer à l'appui de leurs requêtes respectives avoir fait l'objet d'une mesure concrète de surveillance. Pour les mêmes raisons, elle considère que la simple existence de la législation litigieuse constitue en soi une ingérence dans l'exercice par les intéressés des droits découlant de l'article 8 de la Convention. En conséquence, la Cour rejette l'exception du Gouvernement tirée du défaut de qualité de victime des requérants.

2. Sur la justification de l'ingérence

a) Arguments des parties

i. Accessibilité du droit interne

147. Les requérants considèrent que la législation nationale sur la surveillance secrète ne satisfait pas aux exigences de qualité requises pour constituer une « loi », au sens de la Convention, et qu'il y a eu par conséquent violation de l'article 8 de la Convention à leur égard. Ils exposent que même si les attributions générales des services de l'État chargés d'effectuer la surveillance sont réglementées par les lois régissant lesdits services, les différentes mesures d'interception font l'objet de dispositions détaillées qui revêtent un caractère confidentiel. Ils indiquent que cette réglementation est consécutive à la protection dont bénéficient les méthodes d'action des services secrets ainsi que les mesures appliquées par ceux-ci. Ils expliquent que, d'un côté, la législation pertinente habilite les chefs des différents services concernés à réglementer lesdites méthodes et mesures par voie d'arrêtés et que, de l'autre, les tentatives effectuées jusque-là par le législateur en vue de réglementer l'ensemble des questions y afférentes dans une loi unique n'ont pas abouti.

148. Le Gouvernement soutient que la législation litigieuse satisfait aux exigences d'« accessibilité » et de « prévisibilité ». Il avance que l'ensemble des lois nationales pertinentes ont fait l'objet d'une publication au journal officiel, et qu'elles sont par conséquent « accessibles ». Il ajoute que les dispositions desdites lois sont libellées avec suffisamment de précision et d'une manière qui permet à tout individu -- le cas échéant avec des conseils appropriés -- de réguler sa conduite. Il considère que la législation nationale en question donne aux citoyens, de manière claire et détaillée, une indication adéquate quant aux circonstances dans lesquelles les autorités publiques sont habilitées à recourir à la surveillance secrète.

ii. Champ d'application des mesures de surveillance

149. Les requérants considèrent que le champ d'application de la surveillance secrète est vaste. Ils expliquent, à cet égard, que plusieurs services de police et de renseignement peuvent appliquer la mesure en question et qu'ils peuvent le faire relativement à une quantité importante d'infractions, dont certaines, affirment-ils, sont relativement mineures. Ils ajoutent que les services compétents de la police et de la police militaire peuvent, de surcroît, conserver des données de communication aux fins de la prévention et de la découverte de n'importe quelle infraction, sous la seule réserve que celle-ci soit réprimée par la législation nationale. Ils arguent, en outre, que les dispositions énonçant les catalogues d'infractions pour lesquelles une surveillance secrète peut être mise en place ont fait l'objet d'un examen de la Cour constitutionnelle et que celle-ci a conclu dans l'arrêt K 23/11 (précité) à la non-conformité de certaines d'entre elles à la Constitution.

150. Les requérants soutiennent par ailleurs que la procédure « d'urgence » prévue à l'article 19 alinéa 3 de la loi sur la police (paragraphe 35 ci-dessus), selon laquelle la police peut procéder à une surveillance sans l'autorisation d'un juge dans la limite de cinq jours, s'applique à l'ensemble des infractions pour lesquelles le contrôle opérationnel est autorisé et non pas aux seules infractions les plus graves.

151. Ils estiment que la législation sur la surveillance secrète comporte des formulations générales, arguant que selon les termes de l'article 9 de la loi anti-terrorisme (paragraphes 52-57 ci-dessus), cette loi permet aux autorités de recourir à pareille surveillance en cas de « soupçons qu'un ressortissant étranger puisse être impliqué dans des activités terroristes », et que le caractère vague de cette formulation conduirait n'importe qui à s'interroger sur son application en pratique par les services de l'État compétents en la matière.

152. Ils exposent en outre que le degré de précision des dispositions réglementant les attributions en matière de surveillance secrète des différents services de police et de renseignement varie selon le service en cause. Renvoyant à l'article 6 § 8 de la loi sur l'ABW, ils allèguent que celui-ci permet le recours aux techniques de renseignement électronique (*wywiad elektroniczny*) des services de l'ABW, quand bien même les techniques en question ne feraient, selon eux, l'objet d'aucune réglementation spécifique dans le droit national.

153. Ils estiment également que la législation nationale ne précise pas suffisamment les infractions qui peuvent donner lieu à la conservation de données de communication. Selon eux, il découle de la formulation des dispositions législatives en question qu'il peut être recouru à une telle mesure dans n'importe quelle enquête et relativement à n'importe quelle infraction. Ils considèrent que bien que la conservation de données de communication soit autorisée dans les limites des

attributions respectives de chacun des services de l'État concernés, son application n'est pas exempte d'abus de leur part compte tenu de l'absence d'un quelconque mécanisme de contrôle indépendant vis-à-vis des services de l'État en question qui interviendrait au stade de l'autorisation de ladite mesure. Renvoyant aux dispositions pertinentes de la loi sur le CBA, ils ajoutent que les services de cet organe peuvent procéder à une conservation de données de communication à des fins purement analytiques.

154. Ils avancent que la loi sur la police et les autres lois réglementant la surveillance ne définissent pas précisément quelles données de communication peuvent être recueillies, mais renvoient à cet égard à d'autres lois, dont celles sur les télécommunications, sur l'Internet et sur les communications postales, respectivement. Ils indiquent en outre que les lois pertinentes imposent que les données soient conservées par les prestataires de services de télécommunication pendant douze mois, ce qui implique, selon eux, que la quantité des données ainsi mises à disposition des autorités intéressées est très importante.

155. Concernant les catégories de personnes qui peuvent faire l'objet d'une surveillance secrète, les requérants expliquent que l'article 19 § 5 de la loi sur la police prévoit que cette mesure peut être appliquée « y compris » à l'endroit d'un suspect ou d'un accusé, et ils en déduisent que les personnes dont la communication est interceptée ne doivent pas nécessairement être soupçonnées d'avoir commis une quelconque infraction. Renvoyant aux constats de l'arrêt K 23/11 de la Cour constitutionnelle précité, ils arguent que le champ d'application *ratione personae* de la surveillance est, en principe, illimité, ajoutant que la réglementation relative à la conservation de données de communication ne contient, quant à elle, aucune précision quant à son champ d'application *ratione personae*.

156. Les requérants exposent enfin que la législation litigieuse n'énonce aucune dérogation en matière de surveillance des communications professionnelles des avocats et des journalistes. Ils expliquent, d'une part, que même si la loi sur la police impose aux services de l'État ayant effectué une surveillance de procéder à la destruction des informations de ce type qui ont été collectées par eux, elle ne prévoit pas pour autant de mécanisme de contrôle externe et indépendant concernant la mise en œuvre par lesdits services de l'obligation en question et, d'autre part, que seuls les agents des services procédant à la surveillance décident de l'éventuelle suppression des informations collectées en fonction de l'analyse de leur contenu. Ils arguent que ce n'est qu'en cas de transmission pour examen des éléments couverts par le secret professionnel au tribunal compétent que celui-ci décide de l'éventuelle utilisation comme preuve de ces éléments dans une procédure pénale. Ils considèrent, en outre, que le risque de voir les autorités s'emparer du contenu des communications professionnelles des avocats est, en lui-même, de nature à nuire aux droits de la défense des clients de ceux-ci et à la bonne marche de la justice dans son ensemble.

157. Le Gouvernement soutient qu'il découle des dispositions pertinentes des lois réglementant le fonctionnement des services de police et de renseignement que les services concernés recourent aux mesures de surveillance uniquement dans le cadre de leurs attributions respectives et aux fins de la prévention et de la détection des infractions les plus graves, telles qu'elles sont précisément indiquées dans lesdites dispositions. Il ajoute qu'en conséquence de l'arrêt K 23/11 de la Cour constitutionnelle les dispositions des lois censurées par la haute cour ont été amendées, de sorte que l'obligation de procéder à la destruction des éléments couverts

par le secret de la défense et de la confession collectés dans le cadre d'une surveillance s'applique dorénavant à l'ensemble des services de police et de renseignement procédant à celle-ci.

iii. Durée de la surveillance

158. Les requérants arguent que la durée de dix-huit mois pendant laquelle la surveillance secrète peut être mise en place est, en soi, une période longue, et que de surcroît, dès lors que ce sont les services de l'ABW ou de SKW qui y ont recours, ladite mesure peut être renouvelée indéfiniment. Ils ajoutent qu'en cas d'urgence, une mesure de surveillance peut être appliquée pendant cinq jours sans aucune autorisation judiciaire préalable et hors de tout contrôle judiciaire. Ils précisent enfin que la loi anti-terrorisme permet aux autorités de surveiller en secret un étranger sans autorisation judiciaire, pendant une durée pouvant aller jusqu'à trois mois.

159. Le Gouvernement indique que la surveillance est autorisée pour une période n'excédant pas trois mois, et qu'elle ne peut être prolongée qu'une seule fois, sur autorisation du tribunal régional compétent et pour une période maximale de trois mois, si les raisons qui ont justifié sa mise en place n'ont pas cessé d'exister. Il explique qu'en cas de survenance de circonstances nouvelles qui justifient la poursuite de l'enquête, le tribunal compétent peut ordonner le maintien de la surveillance pendant plusieurs périodes consécutives dont la durée totale ne peut excéder douze mois. Il précise, d'une part, que ces règles s'appliquent également en cas d'urgence et, d'autre part, que la surveillance est interrompue aussitôt que les raisons qui ont justifié son application ont cessé d'exister et au plus tard à l'issue de la période pour laquelle elle avait été autorisée.

iv. Autorisation des mesures de surveillance

160. Les requérants exposent que le recours au contrôle opérationnel par les services de l'État compétents requiert l'autorisation préalable d'un tribunal, sauf en cas d'urgence, où la mesure en question peut être mise en place sans autorisation judiciaire dans la limite de cinq jours. Ils indiquent également que l'exigence d'autorisation judiciaire préalable ne s'applique pas à la mesure de conservation des données de communication, et que la loi anti-terrorisme permet la réalisation d'une surveillance secrète pendant trois mois sans l'autorisation préalable d'un tribunal.

161. Les requérants considèrent par ailleurs que la procédure d'autorisation juridictionnelle de la surveillance présente des lacunes, lesquelles résultent notamment, selon eux, de son caractère confidentiel ainsi que de l'absence de participation à celle-ci de l'individu visé par la mesure en question. Ils expliquent à cet égard que la décision rendue à l'issue de ladite procédure est confidentielle, qu'elle n'est pas motivée et qu'elle ne peut être contestée que par le seul procureur, à l'exclusion de la personne soumise à la surveillance, ajoutant que la jurisprudence nationale relative à la surveillance secrète est inaccessible au public, et que le tribunal qui a à connaître d'une demande d'autorisation de surveillance statue en fonction des seuls éléments du dossier que les services concernés ont jugé utile de lui communiquer à l'appui de leur demande. Or, d'après les requérants, les éléments statistiques pertinents indiquent que le pourcentage de demandes d'autorisation de surveillance accueillies par les tribunaux se situe aux alentours de quatre-vingt-dix-neuf pour cent de l'ensemble des demandes traitées. Les requérants estiment que dans ces circonstances, n'importe qui devrait s'interroger tant sur l'utilisation à titre uniquement subsidiaire de la surveillance par les

services de police et de renseignement, que sur l'effectivité du contrôle juridictionnel à l'égard de la surveillance en question.

162. Les requérants indiquent en outre que la conservation de données de communication par les services l'État compétents ne dépend d'aucune autorisation judiciaire préalable. Ils considèrent que l'utilisation que lesdits services font de la mesure en question intervient à titre non subsidiaire mais principal et qu'elle n'est soumise à aucun contrôle effectif indépendant. Sur ce point, ils soutiennent que le contrôle exercé par les juridictions régionales sur la base de rapports semestriels que les services de l'État concernés leur soumettent ne répond pas aux exigences de la Convention en la matière, dès lors, selon eux, qu'il est facultatif et insusceptible de conduire à une appréciation adéquate de la « nécessité » et la « proportionnalité » de la surveillance. Ils ajoutent que la législation pertinente ne précise ni les critères à l'aune desquels ledit contrôle est opéré, ni ses répercussions à l'égard des données recueillies et des personnes visées par la mesure. Ils en déduisent que la conservation de données de communication ne fait pas l'objet d'un contrôle effectif par un organe indépendant qui serait à même de vérifier si la police utilise ses pouvoirs d'une manière raisonnable et conforme aux bonnes pratiques d'enquête.

163. Les requérants avancent également que le contrôle exercé par les procureurs à l'égard des services de l'État recourant à la surveillance ne peut être considéré comme effectif en raison de l'actuelle subordination des procureurs polonais au ministre de la Justice. Selon eux, des considérations similaires s'appliquent à la commission parlementaire supervisant les activités des services spéciaux. Sur ce point, ils arguent que même si cette commission possède une vaste expertise en la matière, elle est composée uniquement d'hommes politiques, à l'exclusion de tout expert, et qu'en outre, ses rapports à l'attention du Parlement sont confidentiels et ses réunions sont tenues à huis clos. Ils ajoutent que la Chambre suprême de contrôle (la « NIK ») n'est pourvue, quant à elle, d'aucune attribution en matière de supervision des mesures de surveillance instaurées à l'égard de personnes privées.

164. Le Gouvernement expose qu'en droit polonais, le contrôle opérationnel fait objet d'un contrôle judiciaire *a priori* relativement à la fois à son autorisation et à sa prolongation, et que la mesure de conservation de données de communication est soumise à un contrôle juridictionnel *a posteriori*. Il allègue que la procédure d'autorisation des mesures de surveillance fait l'objet d'une réglementation détaillée. À cet égard, il explique que les mesures en question peuvent être autorisées par un tribunal régional compétent sur saisine du responsable en chef d'un ou plusieurs services de l'État concernés, de ses adjoints ou d'autres fonctionnaires expressément habilités par les lois pertinentes, lesquels doivent lui soumettre une demande écrite, dûment motivée et préalablement approuvée par un procureur, et que celle-ci doit de surcroît préciser le numéro du dossier concerné, l'infraction en cause et sa qualification juridique, les circonstances justifiant le recours à la surveillance, les éléments prouvant que les autres moyens d'enquête se sont révélés inefficaces ou inutiles, les coordonnées de la personne visée permettant de l'identifier de manière non équivoque, le lieu où la surveillance sera mise en place ainsi que le type, le but et la durée de la mesure de surveillance envisagée. Il indique en outre que le tribunal appelé à statuer sur pareille demande contrôle le caractère régulier et la proportionnalité de la mesure en question, soulignant que l'ensemble des actes du tribunal

compétent sont accomplis dans le respect des dispositions réglementant la transmission, le stockage et la destruction d'informations classifiées. Il ajoute que le rejet de la demande d'autorisation par un tribunal peut donner lieu à un recours de la part de l'autorité publique qui en a fait la demande. Il précise par ailleurs, d'une part, que ce n'est qu'exceptionnellement, en cas d'extrême urgence due à un risque de perte ou d'altération d'éléments de preuve de la commission d'une infraction pénale, que le responsable en chef du service de l'État concerné peut ordonner la mise en place d'une mesure de surveillance sur la base de la seule autorisation préalable du procureur compétent et, d'autre part, que si l'autorisation juridictionnelle relative à ladite mesure n'intervient pas dans les cinq jours suivant le début de son application, la surveillance est interrompue et les informations obtenues dans ce cadre sont détruites sans délai.

165. Le Gouvernement indique également que l'article 20 ca de la loi sur la police (paragraphe 49 ci-dessus) impose à la police l'obligation de soumettre à la juridiction régionale compétente un rapport semestriel contenant les informations suivantes, relativement à la conservation et au traitement de données de communication au cours de la période de référence: le nombre de cas de conservation de données, avec l'indication du type de donnée en question ; les qualifications juridiques en relation avec lesquelles les demandes de conservation de données de communication ont été introduites, ou des informations concernant la conservation de données visant à la protection de vies humaines et de la santé ou en soutien de missions de recherche ou de sauvetage. Il ajoute que le tribunal qui contrôle l'application de la mesure de conservation de données de communication par les services de l'État compétents peut prendre connaissance du contenu de ces rapports, et qu'il informe la police de ses conclusions dans un délai de trente jours à compter de la fin de celui-ci. Il précise que ce mécanisme de contrôle de la conservation de données de communication a été instauré à la suite de l'arrêt K 23/11 de la Cour constitutionnelle et de l'entrée en vigueur, consécutive audit arrêt, de la loi du 15 janvier 2016.

166. Il expose, en outre, que la conservation et le traitement des données de communication par les services de l'État ayant recours à cette mesure de surveillance se font sous la supervision des responsables respectifs de ceux-ci, à tous les stades du processus y affèrent. Il explique que la mesure de surveillance en question constitue pour les services de l'État concernés un mode de recherche à la fois principal et subsidiaire, précisant qu'en ce qui concerne les enquêtes menées relativement à certaines infractions telles que le harcèlement (stalking), la fraude commise *via* Internet ou la diffusion d'images à caractère pornographique, elle est, en pratique, l'unique moyen pour eux de se procurer des éléments de preuve pertinents.

167. Il argue que le caractère secret de la surveillance est un gage d'efficacité des services de l'État y ayant recours, et qu'en conséquence la mesure en question n'est pas notifiée à la personne qui en fait l'objet.

168. Il fait enfin observer que l'application des mesures de surveillance est non seulement soumise à un contrôle juridictionnel, mais qu'elle fait en plus l'objet d'une supervision de la part du Parlement ou, concernant les activités des services spéciaux, de la commission parlementaire, laquelle, indique-t-il, examine les rapports annuels que les responsables en chef respectifs des services concernés lui soumettent. Il ajoute que ces derniers, dès lors qu'ils agissent dans l'exercice de leurs fonctions officielles, font en outre l'objet d'une supervision de la NIK sous l'angle de la légalité, de l'efficacité et de la diligence de la mesure ainsi qu'à l'aune de la prudence économique. Il

explique par ailleurs que selon l'article 231 §§ 1 et 2 du CP, un abus de pouvoir commis par un agent public dans l'exercice de ses fonctions officielles est passible d'une peine d'emprisonnement de trois ans, ou de dix ans si l'agent mis en cause a agi avec l'intention de se procurer un avantage financier ou personnel, précisant que cette disposition s'applique à l'ensemble des agents des services de l'État ayant recours à la surveillance.

v. Procédure à suivre pour la consultation, l'utilisation, la conservation et la destruction des données interceptées

169. Les requérants soutiennent que les tribunaux nationaux n'interviennent aucunement dans la procédure de destruction d'éléments issus d'une surveillance secrète qui sont sans utilité pour une enquête pénale, et que les dispositions réglementant la destruction des informations couvertes par le secret professionnel ne garantissent pas que la police ou les services secrets n'auront pas accès à ces informations, alors que, de leur avis, celles-ci nécessiteraient une protection accrue. Ils arguent que la destruction par les services de police et de renseignement des données de communication conservées n'est soumise à aucun contrôle de la part d'un organe indépendant des services qui les ont recueillies, ajoutant que la législation pertinente ne précise pas si le tribunal qui exerce le contrôle de la conservation de données de communication est habilité à ordonner la destruction des données inutiles ou illicites.

170. Ils indiquent en outre que si à l'issue de la surveillance secrète, les services de l'État compétents n'ont recueilli aucune preuve de la commission d'une infraction, l'individu visé par ladite mesure n'est pas informé de celle-ci, et ils font observer qu'il ne peut par conséquent pas en faire contrôler la légalité. Ils considèrent que pareille situation est contraire aux conclusions tant de la Cour constitutionnelle dans sa décision S 2/06 (paragraphe 72 ci-dessus) que de la Commission de Venise (paragraphe 92 ci-dessus), lesquelles conclusions n'ont, selon eux, jamais été mises en œuvre par le Gouvernement polonais. Renvoyant aux éléments statistiques pertinents en leur possession, ils ajoutent que le nombre de dossiers pénaux dans lesquels les informations collectées dans le cadre d'une surveillance ont été utilisées comme preuve est faible.

171. Les requérants affirment par ailleurs que l'ensemble des préoccupations qu'ils ont exposées concernant le défaut d'efficacité du contrôle des mesures de surveillance secrète ont été corroborées lors du récent scandale autour du programme « Pegasus »,[38] aucune des victimes alléguées de la surveillance effectuée à l'aide du programme en question ne disposant, selon eux, d'un quelconque moyen de vérifier si ladite surveillance avait eu lieu et si elle était régulière. Ils considèrent que cette situation constitue un argument de plus en faveur de l'instauration d'une obligation de notification de la mesure de surveillance à la personne qui y a été soumise.

172. Le Gouvernement indique quant à lui que les éléments qui ont été obtenus dans le cadre de mesures opérationnelles d'investigation et qui n'ont pas donné lieu à des poursuites ou ne sont pas pertinents pour des poursuites en cours sont détruits sans délai par une commission protocolaire en application d'une décision prise par l'autorité de police qui a sollicité l'autorisation de recourir aux mesures en question. Il ajoute que les autorités compétentes, à savoir le commandant en chef de la police nationale et ses homologues des services spéciaux concernés, ordonnent sans délai la destruction par une commission protocolaire des éléments recueillis au moyen d'une surveillance qui contiennent les informations visées à l'article 178 du

CPP (paragraphe 58 ci-dessus). Il expose en outre qu'en cas de collecte par les services procédant à la surveillance secrète d'éléments de preuve justifiant l'engagement de poursuites pénales ou s'avérant pertinents à l'égard de poursuites pénales en cours, les preuves en question sont transmises au procureur général ou au procureur régional compétent avec l'ensemble des éléments résultant des mesures opérationnelles d'investigation. Il précise que les informations couvertes par le secret professionnel (qui sont définies à l'article 178a du CPP (*ibidem*)) sont transmises au procureur, puis au tribunal qui avait autorisé la surveillance, en vue d'une décision sur ce qu'il convient d'en faire. Il explique, sur ce point, que le tribunal, statuant sans délai, autorise l'utilisation dans une procédure pénale des informations couvertes par le secret professionnel dès lors qu'il estime que « l'intérêt de la bonne administration de la justice l'exige » et qu'un fait pertinent pour la procédure concernée ne peut être établi au moyen d'une autre preuve, et qu'il ordonne la destruction de celles dont utilisation dans une procédure pénale n'est pas permise ou qui sont inutiles à une telle procédure.

173. Le Gouvernement soutient par ailleurs que la conservation de données de communication par les services de police et de renseignement fait l'objet d'une réglementation rigoureuse prévue par la législation pertinente. Il indique qu'en règle générale, les prestataires des services TIC sont tenus de donner aux agents de police compétents un accès aux données de ce type. Il explique que pour assurer un contrôle interne concernant cette mesure de surveillance, les responsables en chef des services spéciaux, leurs homologues de la police nationale et ceux des autres organismes habilités à l'appliquer tiennent des registres électroniques confidentiels dans lesquels sont consignées toutes les demandes d'accès aux données de communication. Il ajoute, d'une part, que les données indiquées à l'article 20 ca de la loi sur la police (paragraphe 49 ci-dessus) qui sont utiles pour une procédure pénale en cours d'instruction sont communiquées par les agents de police habilités au procureur compétent, lequel décide ce qu'il convient d'en faire, et, d'autre part, que les données de communication qui sont sans utilité pour une procédure pénale sont détruites sans délai par une commission protocolaire. Il précise que les opérateurs des services TIC sont tenus par une obligation de conserver les données de communication collectées par eux pendant douze mois.

b) Observations des tiers intervenants

i. Le Commissaire aux droits de l'homme de la République de Pologne

174. Le Commissaire aux droits de l'homme considère que si les opérations de surveillance doivent, certes, rester secrètes, elles ne devraient pas pour autant être réalisées à l'abri de tout contrôle externe indépendant. Il estime que les personnes soumises à une surveillance devraient pouvoir faire contrôler la légalité de celle-ci par une instance indépendante des services de l'État qui l'appliquent, et soutient que les amendements législatifs mentionnés au paragraphe 9, qui étaient censés mettre la législation pertinente en conformité avec les normes dégagées par la Cour constitutionnelle, ont rendu la réglementation applicable encore plus attentatoire aux normes en question.

175. Faisant état des principaux éléments qui, d'après lui, suscitent l'inquiétude quant à la législation en question, le Commissaire aux droits de l'homme expose ce qui suit : premièrement, elle n'énonce pas de délais maximum de surveillance autorisée, ou alors, quand c'est le cas, les délais

prévus sont trop longs ; deuxièmement, le catalogue des infractions pour lesquelles la mise en place de la surveillance peut être autorisée est trop large ; troisièmement, la réglementation de l'utilisation en tant que moyens de preuve dans une procédure pénale des éléments couverts par le secret professionnel qui ont été obtenus au moyen d'une surveillance est imprécise ; quatrièmement, les services de l'État procédant à la surveillance ont en permanence un accès quasi-illimité aux données de communication, lequel, selon lui, ne fait l'objet d'aucun contrôle ; cinquièmement, les services de l'État en question ne sont tenus par aucune obligation en matière de notification de ladite mesure à la personne visée par celle-ci ; sixièmement, la personne soumise à la surveillance ne dispose d'aucun recours qui lui permettrait, le cas échéant, de faire établir l'existence d'une surveillance la concernant et d'en faire contrôler la légalité. Renvoyant par ailleurs aux éléments statistiques pertinents en sa possession, le Commissaire aux droits de l'homme ajoute qu'en Pologne, le nombre de demandes d'autorisation de surveillance reste élevé et que le pourcentage de rejets de celles-ci est faible.

176. Il stigmatise tout particulièrement la loi anti-terrorisme, estimant qu'elle est imprécise et discriminatoire vis-à-vis des ressortissants étrangers. Il argue, d'une part, que la surveillance mise en place en application de ladite loi échappe à tout contrôle externe et, d'autre part, que les pouvoirs dévolus au chef de l'ABW pour fixer par arrêté confidentiel le catalogue des données que les services placés sous sa supervision peuvent collecter dans le cadre d'une surveillance sont larges. Il fait part de ses préoccupations quant à l'absence d'un recours qui permettrait aux personnes visées par la surveillance de faire contrôler la légalité de celle-ci. Il explique, en outre, qu'en cas d'inscription, consécutive à une mesure de surveillance, de la personne qui fait l'objet de celle-ci à son insu au registre des individus soupçonnés d'être impliqués dans des activités terroristes, la personne concernée n'est jamais informée de ce fait et elle n'a donc pas la possibilité de demander que les informations collectées à son insu soient rectifiées ou effacées du registre en question.

177. Le Commissaire aux droits de l'homme fait par ailleurs observer que l'article 168a du CPP permet l'utilisation par les autorités diligentant une procédure pénale des éléments de preuve collectés dans le cadre d'une surveillance mise en place illégalement à l'égard d'une personne privée.

ii. Fondation ePaństwo

178. La tierce intervenante indique qu'elle est spécialisée dans le domaine des nouvelles technologies et qu'elle œuvre pour l'ouverture et la transparence des données numériques ainsi que pour le libre accès à celles-ci. En l'espèce, elle fait part de ses préoccupations quant aux insuffisances du contrôle auquel sont soumis les services de police et de renseignement polonais qui ont recours à la surveillance secrète. Elle considère que le champ d'application *ratione personae* de cette surveillance est large, dès lors qu'en sus des ressortissants polonais, elle peut être mise en place à l'égard des étrangers et de n'importe quel individu qui est en contact avec eux. Elle ajoute que l'actuel gouvernement polonais entretient une attitude hostile envers les ONG engagées pour la défense des droits humains et elle estime par conséquent que celles-ci courent un risque accru de faire elles-mêmes l'objet d'une surveillance secrète.

iii. Fair Trials International

179. Le tiers intervenant Fair Trials International expose que les autorités diligentant des enquêtes relativement aux infractions liées au terrorisme et à la récente crise du Covid-19 ont fréquemment recours à la surveillance à l'égard de personnes privées de leur liberté, et ce d'une manière qu'il estime problématique au regard des exigences de l'article 6 de la Convention. Il-prône l'interdiction de l'utilisation par les autorités en question des éléments de preuve collectés par elles en violation du droit au respect de la vie privée des personnes accusées d'une infraction pénale, arguant que la législation polonaise actuellement en vigueur n'offre pas à celles-ci de garanties de protection suffisantes à cet égard. Il insiste tout particulièrement sur la nécessité d'un contrôle *a priori* et *a posteriori* de la surveillance, compte tenu du caractère intrusif de celle-ci pour les personnes qui en font l'objet. Il considère que le contrôle des mesures de surveillance de ce type doit être particulièrement robuste et nécessairement juridictionnel, précisant que sont impératives, à cet égard, tant la notification de ladite mesure à la personne qui y a été soumise que l'instauration d'un recours propre à permettre à celle-ci de faire contrôler la légalité de cette surveillance. Il ajoute qu'en l'absence en droit national de dispositions réglementant ces problématiques, le contrôle de la légalité et de la conformité de la surveillance secrète au principe de l'État de droit dans une démocratie et aux normes pertinentes en matière de protection de la vie privée devrait être confié à un organisme indépendant des services de l'État appliquant ladite mesure.

180. Le tiers intervenant soutient en outre que le cadre juridique de la surveillance doit être clair, prévisible et pourvu de garanties spécifiques concernant la protection du secret des communications des avocats et de leurs clients. S'appuyant sur les conclusions des enquêtes qu'il a menées en la matière, il indique que l'assistance juridique aux personnes accusées d'une infraction pénale qui sont privées de leur liberté est actuellement assurée en majeure partie par voie de moyens de communication électroniques, ce qui corrobore, selon lui, l'argument tiré d'un besoin de protection accrue contre l'interception abusive de communications de ce type.

iv. La Commission internationale de juristes (« la CIJ »)

181. Renvoyant aux standards relatifs, respectivement, à la confidentialité des échanges entre les avocats et leurs clients et à la surveillance secrète des personnes privées, tels qu'ils résultent de la jurisprudence de la Cour européenne des droits de l'homme et de la CJUE ainsi que des travaux de différentes instances internationales, parmi lesquelles le Haut-commissaire des Nations Unis pour les droits de l'homme et le Rapporteur spécial pour la liberté d'expression de la commission interaméricaine des droits de l'homme, la tierce intervenante considère que la surveillance de masse représente actuellement la menace la plus grave à laquelle sont exposés les individus, d'autant que, selon elle, des garanties suffisamment solides visant à protéger les individus visés contre une surveillance abusive font défaut. Elle ajoute que l'ensemble des communications des avocats avec leurs clients et des militants œuvrant pour les droits de l'homme devraient faire l'objet d'une protection accrue contre les mesures de surveillance abusives, eu égard aux enjeux des échanges en question pour les intéressés et pour la société démocratique dans son ensemble.

v. Le conseil national des barreaux polonais (le « NRA »)

182. Le tiers intervenant expose qu'en conséquence de l'entrée en vigueur des amendements de la législation pertinente (paragraphe 9 ci-dessus), les communications de tout avocat en Pologne sans aucune exception peuvent être interceptées par les services de l'État compétents en la matière en dehors de tout contrôle, sans que les intéressés le sachent et sans qu'ils puissent dénoncer d'éventuels abus de la part desdits services de l'État. Il estime qu'il ne fait aucun doute que la haute performance des moyens techniques actuels dont disposent les services de police et de renseignement concernés leur permet de se procurer en quantité quasi illimitée toutes sortes d'informations sur les individus, y compris concernant la vie privée des avocats.

183. Il soutient que les services de police et de renseignement traitent les éléments qu'ils collectent dans le cadre d'une surveillance à l'insu des personnes visées également à des fins opérationnelles, lesquelles n'ont aucun rapport avec une quelconque procédure en cours d'instruction. Il explique qu'en cas de recueil par les services de l'État en question des informations couvertes par le secret professionnel qui sont précisées à l'article 178 du CPP, celles-ci devraient – à tout le moins en théorie – être détruites par eux sans délai. Or, de son avis, il est évident qu'une fois que les services de l'État concernés ont pris connaissance de leur contenu, ils sont réticents à s'en débarrasser complètement. Le tiers intervenant exprime par ailleurs des préoccupations quant au fait que l'agent qui procède à la surveillance soit le seul à décider s'il convient de détruire ou de conserver les éléments ainsi collectés, estimant que pareille situation conduit nécessairement à s'interroger quant au respect de la confidentialité des échanges entre les avocats et leurs clients par les services de l'État concernés.

184. Le tiers intervenant considère en outre que la qualité de la législation relative à la surveillance secrète est sujette à caution, ce pour les raisons suivantes. Premièrement, la législation incriminée concernerait plus de cinquante infractions réprimées, selon le cas, par le code pénal polonais ou par l'une des sept lois relatives, respectivement, aux services de police et de renseignement compétents. Deuxièmement, l'individu visé par une mesure de surveillance ne disposerait d'aucun moyen propre à lui permettre de faire contrôler la finalité de protection de la sécurité publique que doit poursuivre la surveillance en question. Troisièmement, les dispositions autorisant la mise en place d'une surveillance à l'égard de personnes privées en cas de « soupçons » de la commission par elles d'une infraction seraient imprécises et encourageraient un recours arbitraire à ladite mesure de la part des organismes compétents en la matière. Quatrièmement, les dispositions énonçant le droit pour les services de l'État habilités de mettre en place une surveillance dès lors que les autres méthodes d'investigation se sont révélées infructueuses au regard de but recherché par eux ou sont dépourvues d'utilité seraient également imprécises à un point tel qu'elles conféreraient auxdits services une marge d'appréciation quasi illimitée en la matière.

185. Le tiers intervenant estime enfin que l'étendue des pouvoirs des tribunaux dans les procédures de contrôle des services de l'État ayant recours à la surveillance est insuffisante. Il argue que la destruction des éléments collectés dans le cadre d'une surveillance effectuée en application des dispositions relatives aux situations urgentes ne fait l'objet d'aucun contrôle externe aux services de l'État concernés, ajoutant qu'il en va de même des éléments recueillis qui relèvent du secret professionnel des avocats.

vi. Privacy International, Article 19 et Electronic Frontier Foundation

186. Les organisations intervenantes considèrent que la distinction qui était opérée jusqu'ici entre la conservation de données de communication, d'une part, et l'interception de données se rapportant au contenu des communications, d'autre part, concernant le degré d'intrusion de la surveillance dans la sphère privée des personnes visées est désormais dépourvue de pertinence. Elles estiment que le premier de ces modes de surveillance s'apparente à une surveillance de masse et qu'il devrait par conséquent toujours être entouré de garanties suffisamment solides en vue de la protection des individus contre d'éventuels abus. Selon elles, l'accès direct et illimité des services de l'État compétents en la matière aux données de communication constitue une ingérence très poussée dans la sphère privée des personnes soumises à ladite mesure. Il est donc impératif, à leurs yeux, de faire en sorte que ce mode de surveillance particulier soit appliqué uniquement dans des situations prévues de manière précise par la loi, et sous réserve d'une autorisation préalable émanant d'un organisme indépendant des services ayant recours à la mesure en question. Elles ajoutent que les garanties minimales de protection contre les éventuels abus en la matière devraient englober un mécanisme de contrôle indépendant, impartial, doté de ressources suffisantes et propre à assurer la transparence de la surveillance mise en place ainsi que la mise en jeu, le cas échéant, de la responsabilité d'agents auteurs d'abus.

187. Les tierces intervenantes indiquent par ailleurs que l'on observe un consensus croissant au sein des pays démocratiques relativement à une exigence de notification aux personnes soumises à une surveillance de la mesure en question aux fins d'une éventuelle contestation par elles de sa régularité. Elles considèrent que cette exigence ne devrait subir d'exception que dans les cas où une notification serait susceptible de compromettre la finalité de la surveillance ou de mettre en danger la vie d'individus. En outre, selon elles, compte tenu du possible effet inhibiteur de la surveillance sur la société civile, l'ensemble des ONG sans aucune exception devraient jouir, contre les surveillances abusives, d'une protection analogue à celle dont bénéficient les avocats et des journalistes.

vii. Le Rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (« le Rapporteur spécial »)

188. Le Rapporteur spécial expose que dans le cadre de ses missions, il entretient un dialogue régulier avec les agences de renseignement et de sécurité. Il indique qu'il a présenté au Conseil des droits de l'homme plusieurs rapports,[39] dont une compilation des bonnes pratiques concernant la surveillance et relatives aux cadres et aux mesures juridiques et institutionnels, et notamment au contrôle, qu'il estime pertinents aux fins de garantie du respect des droits de l'homme par les services de renseignement dans la lutte antiterroriste[40].

189. Le Rapporteur spécial fait observer que le rythme soutenu du développement technologique, grâce auquel de plus en plus de personnes à travers le monde peuvent utiliser les nouvelles technologies de l'information et des communications, permet aussi aux pouvoirs publics, aux entreprises et aux personnes privées de surveiller, d'intercepter et de collecter plus facilement des données, ce qui peut engendrer des violations des droits de l'homme, dont en particulier du

droit à la vie privée. Il ajoute que la tendance à la « datafication », à savoir l'utilisation généralisée et à grande échelle de la collecte de données dans le cadre du travail des services de renseignement, crée des défis évidents en matière de droits de l'homme et d'État de droit.

190. Le Rapporteur spécial considère qu'eu égard à l'importance croissante du renseignement et du caractère secret de la surveillance, il est indispensable qu'un mécanisme de contrôle portant sur chaque étape du processus d'application de ce type de mesure soit mis en place pour prévenir d'éventuelles violations des droits de l'homme. Il estime que le mécanisme en question devrait être indépendant des autorités chargées de la mise en œuvre de la surveillance, et qu'il devrait inclure l'autorisation judiciaire des mesures en question, la notification *a posteriori* de celles-ci aux personnes visées ainsi qu'un recours permettant aux individus dont les droits ont été violés en conséquence de ladite mesure d'obtenir réparation du tort subi. Il précise en outre que les mesures de surveillance mises en place à l'égard de membres des professions légales ou d'organisations de la société civile et à l'insu de ceux-ci devraient s'accompagner de garanties de protection particulièrement solides contre d'éventuels abus commis par des agences du renseignement.

191. Le Rapporteur spécial estime enfin que la notification *a posteriori* des mesures de surveillance aux personnes qui en font l'objet constitue le moyen le plus adéquat tant pour permettre à la personne concernée de se défendre vis-à-vis des autorités y ayant eu recours que pour donner aux organismes qui supervisent ces autorités la possibilité de mener convenablement leurs missions en la matière. Se référant, à cet égard, aux conclusions pertinentes de l'Agence européenne des droits fondamentaux,[41] il indique que dans six États membres de l'Union européenne, les personnes visées par la surveillance sont informées de celle-ci *a posteriori* et que dans dix-neuf autres États membres, l'obligation de notification existe sous conditions, à l'instar du droit de la personne visée par la surveillance d'accéder aux informations collectées à son insu dans le cadre de la mesure en question.

c) Appréciation de la Cour

i. Le contrôle opérationnel

α) Principes généraux

192. Les principes généraux pertinents concernant la question de savoir quand des mesures secrètes de surveillance, y compris l'interception de communications, peuvent être justifiées au titre de l'article 8 § 2 de la Convention ont été exposés en détail dans l'arrêt *Roman Zakharov* (précité, §§ 227-34, 236, 243, 247, 250, 257-58, 275, 278 et 287-88). Nombre de ces principes ont été récemment réitérés – bien que dans un contexte quelque peu différent – l'interception de masse – dans les arrêts *Centrum för rättvisa*, §§ 246-53, et *Big Brother Watch et autres,* §§ 332-39, tous deux précités).

193. S'il n'est pas nécessaire de les reprendre tous ici, il importe de souligner que l'exigence primordiale en la matière est qu'un système de surveillance secrète doit comporter des garanties effectives – en particulier des mécanismes d'examen et de contrôle – qui protègent contre le risque inhérent d'abus et qui limitent à ce qui est « nécessaire dans une société démocratique » l'ingérence qu'un tel système entraîne dans les droits protégés par l'article 8 de la Convention.

Cela étant, même si la législation applicable contient des dispositions qui délimitent l'étendue des pouvoirs des services de l'État procédant à la surveillance secrète, cela peut ne pas suffire à enrayer le risque de détournement de ce mode d'investigation par les services de l'État en question. C'est pourquoi il conviendrait de compléter les mécanismes de contrôle des opérations de surveillance existants par les dispositifs appropriés susceptibles de garantir que les services de l'État concernés n'outrepassent pas leurs attributions en la matière. S'il n'appartient pas à la Cour d'imposer des solutions précises en la matière aux États contractants ni de se prononcer sur l'opportunité des techniques choisies par eux pour réglementer ces problématiques, il lui paraît opportun d'indiquer qu'un mécanisme de contrôle des opérations de surveillance secrète devrait préférablement s'appuyer sur un organisme de contrôle indépendant agissant de sa propre initiative et possédant les instruments juridiques nécessaires pour détecter les abus et lutter contre eux. Il serait souhaitable que l'organe de contrôle en question soit habilité à consulter toutes les informations, même classées, et soit doté de pouvoirs d'investigation et des compétences nécessaires, notamment, pour pouvoir ordonner la cessation d'une interception irrégulière et la destruction des éléments interceptés obtenus et/ou conservés de manière illégale (voir, *mutatis mutandis*, *Centrum för rättvisa*, précité, § 273).

194. Dans des affaires telles que la présente espèce, où les requérants se plaignent de manière abstraite d'un système de surveillance secrète, et non pas de cas d'application spécifiques de pareille surveillance, les lois et pratiques nationales pertinentes doivent être examinées telles qu'elles se présentent au moment où la Cour examine la recevabilité de la requête, plutôt que telles qu'elles étaient au moment de l'introduction de celle-ci. De plus, l'appréciation de la question de savoir si les lois en cause offrent des garanties effectives doit se fonder non seulement sur les lois telles qu'elles existent dans le corpus législatif, mais aussi sur a) le fonctionnement effectif du régime de surveillance et b) l'existence ou l'absence de preuves d'abus réels (voir, *idem*, §§ 151 et 274, et *Big Brother Watch et autres*, §§ 270 et 360, tous deux précités).

β) L'application au cas d'espèce

195. La Cour renvoie à son constat ci-dessus (paragraphe 146) selon lequel la simple existence de la législation incriminée par les requérants constitue en soi une ingérence dans l'exercice par les intéressés des droits découlant de l'article 8 de la Convention. Elle observe qu'en Pologne, les mesures de contrôle opérationnel sont réglementées par une série de lois, parmi lesquelles la loi portant réglementation de la police nationale et celles régissant divers autres services spéciaux de l'État. Elle relève que les parties ne contestent pas que les mesures de surveillance litigeuses en tant que telles ont une base en droit interne, ni que les lois y relatives ont fait l'objet d'une publication officielle et sont accessibles aux citoyens. Prenant note, à cet égard, de l'argument soulevé par les requérants relativement à un manque d'accessibilité de quelques-unes des dispositions encadrant les mesures d'interception, elle considère, d'une part, que l'argument en question est insuffisamment étayé (paragraphe 147 ci-dessus ; pour un raisonnement *a contrario*, voir, *Roman Zakharov* précité, §§ 180 et 241-242) et, d'autre part, qu'il n'y a pas lieu de l'examiner plus avant mais qu'il convient plutôt de se concentrer sur les exigences de « prévisibilité » et « nécessité ». Par ailleurs, il est clair pour la Cour que les mesures de surveillance autorisées en droit polonais poursuivent les buts légitimes que sont, entre autres, la prévention des infractions pénales, la

protection de la sécurité nationale, de la sûreté publique et du bien-être économique du pays. Il reste donc à vérifier si le droit interne contient des garanties et des garde-fous suffisants et effectifs propres à satisfaire aux exigences de « prévisibilité » et de « nécessité dans une société démocratique ».

196. La Cour appréciera donc successivement la portée et la durée des mesures de surveillance secrète, les procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des donnés interceptées, les procédures d'autorisation, les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne (*Roman Zakharov*, précité, §§ 237-238).

– *Champ d'application des mesures de surveillance secrète*

▪ Champ d'application *ratione materiae* de la surveillance secrète

197. La Cour rappelle que le droit national doit définir le champ d'application des mesures de surveillance secrète en fournissant aux citoyens des indications appropriées sur les circonstances dans lesquelles les pouvoirs publics peuvent recourir à de telles mesures – en particulier en définissant les catégories de personnes susceptibles d'être mises sur écoute et en énonçant clairement la nature des infractions susceptibles de donner lieu à un mandat d'interception (*Roman Zakharov*, précité, § 243). Elle souligne que le critère de prévisibilité n'exige toutefois pas des États qu'ils énumèrent lesdites infractions de manière exhaustive. En revanche, ils doivent fournir de précisions suffisantes quant à la nature de celles-ci (*Kennedy c. Royaume-Uni*, (no 26839/05, 18 mai 2010) § 159, *Zakharov*, § 244, précité).

198. En l'espèce, la Cour observe que le champ d'application *ratione materiae* de la surveillance secrète, tel qu'il ressort de la législation litigieuse, a été déterminé différemment pour chacun des services de l'État chargés d'effectuer ladite surveillance. Ainsi qu'il se dégage des dispositions pertinentes, elle note que le domaine d'application de la surveillance secrète est large. Concernant, tout particulièrement, la loi relative à la police nationale, la Cour relève que la loi en question énonce une liste des infractions pouvant donner lieu à la réalisation d'une surveillance secrète. Elle constate toutefois que ladite loi autorise la surveillance pour un très large éventail d'infractions pénales, y compris des délits relativement mineurs. La Cour rappelle dans ce contexte que la surveillance du contenu des communications n'est permise que pour les infractions les plus graves (voir, *mutatis mutandis, Roman Zakharov*, § 245, *Ekimdzhiev et autres*, § 299, *Kennedy* § 159 et *Klass et autres*, § 51, tous précités). Se reportant aux constats exposés dans l'avis de la Commission de Venise précité, la Cour retient que cette instance est parvenue à des conclusions analogues, en indiquant aux autorités nationales que le champ d'application *ratione materiae* de la surveillance devait être circonscrit aux infractions les plus dangereuses.

199. La Cour observe que les catalogues d'infractions pour lesquelles la surveillance opérationnelle peut être effectuée ont été précisés par le législateur au moyen de différentes techniques législatives : en indiquant des passages spécifiques des lois pénales, en précisant les types d'infractions concernées, et parfois en faisant référence à des chapitres entiers ou à des lois spéciales dans lesquels ces infractions étaient spécifiées. Elle considère qu'il ne lui n'appartient

pas de dire quelle technique de rédaction législative est la plus appropriée pour réglementer les problématiques en question. Elle estime que ce qui importe le plus, c'est que les dispositions énonçant un catalogue d'infractions pour lesquelles la surveillance secrète peut être mise en place soient suffisamment prévisibles dans leur application et soient libellées de telle façon que les autorités nationales ne puissent diligenter la mesure en question que pour les infractions suffisamment graves. Ainsi qu'il se dégage des conclusions de l'arrêt K 23/11 de la Cour constitutionnelle (précité), elle relève que le législateur polonais a utilisé parfois des formulations très générales, au point que les cas dans lesquels les autorités pouvaient avoir recours à pareille mesure en pratique pouvait prêter à confusion. Elle note qu'en conséquence des constats à laquelle la haute juridiction est parvenue, quelques-unes des dispositions de la loi sur l'ABW précisant le catalogue d'infractions pour lesquelles la surveillance pouvait être réalisée par l'agence en question ont été écartées en raison de leur manque de clarté, et certaines des dispositions analogues des lois relatives aux autres services de l'État concernés ont été jugées compatibles avec la Constitution sous réserve d'une interprétation conforme aux indications énoncées par la Cour constitutionnelle.

200. La Cour a déjà dit que l'absence de toute précision sur la manière dont il convenait d'interpréter les notions-clés de la législation sur la surveillance secrète était problématique (*ibidem*). En même temps, elle rappelle avoir jugé que l'exigence de « prévisibilité » de la loi ne va pas jusqu'à obliger les États à adopter des dispositions légales énumérant en détail toutes les situations susceptibles de donner lieu à une décision de mise en place d'une opération de surveillance secrète (*Szabó et Vissy c. Hongrie*, no 37138/14, § 64, 12 janvier 2016).

- Champ d'application *ratione personae* de la surveillance secrète

201. Quant à la question de savoir qui peut être visé par la surveillance secrète, la Cour observe qu'il se dégage des constats auxquels la Cour constitutionnelle est parvenue dans l'arrêt K 23/11 (précité) que le champ d'application *ratione personae* de la surveillance est large. Ainsi qu'il ressort de l'avis de la Commission de Venise (précité), elle note en outre que cette instance a indiqué que les catégories de personnes susceptibles de faire l'objet d'un contrôle opérationnel n'étaient pas précisées dans la loi, de sorte que ce pouvait être n'importe quel individu ou groupe pour autant que l'on pût probablement obtenir ainsi des informations utiles au regard du but de la surveillance. À cet égard, la Cour rappelle avoir jugé que les mesures d'interception visant une personne non soupçonnée d'une infraction mais susceptible de détenir des informations sur une telle infraction pouvaient être justifiées au regard de l'article 8 de la Convention (voir, *Greuter c. Pays-Bas* (déc.), no 40045/98, 19 mars 1998, et *Roman Zakharov*, précité, § 245). Elle relève qu'en droit polonais, les demandes d'autorisation de mise en place d'un contrôle opérationnel doivent mentionner précisément la personne visée par la surveillance en question, ce qui implique que la surveillance de ce type est toujours ciblée. Cela étant, la Cour ne perd pas de vue que la législation applicable ne semble pas imposer d'obligations concernant le contenu de la décision portant autorisation de la surveillance. Or elle considère que le cercle de personnes qui sont susceptibles de faire l'objet d'une surveillance secrète devrait être précisé dans la décision en question, et que l'autorité qui octroie l'autorisation devrait suffisamment motiver sa décision sur ce point.

– *La durée des mesures de la surveillance secrète*

202. En l'espèce, la Cour observe que selon la législation pertinente, un juge peut autoriser une mesure d'interception pour une durée n'excédant pas trois mois. Elle retient également qu'une prolongation est possible moyennant une décision de justice pour une période supplémentaire d'un maximum de trois mois, si les motifs initiaux de mise en place de la surveillance sont encore valables. Elle relève, de plus, que dans les cas dûment justifiés, la surveillance peut être prolongée par une juridiction supérieure pour plusieurs périodes consécutives dans la limite d'un total de douze mois. Par ailleurs, la surveillance ne doit pas durer plus de dix-huit mois au total. Elle note en outre que le contrôle opérationnel doit cesser dès que les raisons qui ont justifié sa mise en place ont cessé d'exister et au plus tard à l'expiration de la période pour laquelle il a été autorisé. Au vu de l'ensemble de ces éléments, elle considère que le droit interne indique avec clarté la période maximale au terme de laquelle une autorisation d'interception parvient à expiration et les circonstances dans lesquelles pareille autorisation peut être renouvelée. Elle observe que la durée d'une opération d'interception peut dépendre de plusieurs facteurs, notamment de la gravité des infractions pour lesquelles cette mesure est diligentée, de celle des soupçons qui pèsent sur la personne surveillée et de celle de l'ingérence que la surveillance en question entraîne dans l'exercice par la personne visée de ses droits relevant de la sphère protégée par l'article 8. Elle estime toutefois que compte tenu des lacunes relevées ci-dessous dans le modèle de surveillance secrète considéré, il n'y a pas lieu en l'espèce d'examiner plus avant cette question.

– *Autorisation des interceptions*

203. En ce qui concerne les procédures d'autorisation de la surveillance, la Cour réaffirme que celles-ci doivent être à même de garantir que la surveillance secrète n'est pas ordonnée par hasard, irrégulièrement ou sans examen approprié et convenable (*Roman Zakharov*, précité, § 257). Aux fins de son examen de ce point, elle prendra en compte un certain nombre de facteurs, parmi lesquels, notamment, le service compétent pour autoriser la surveillance, la portée de l'examen qu'il effectue et le contenu de l'autorisation d'interception (*idem*). La Cour rappelle, en outre, que la délivrance d'autorisation par un service non judiciaire aux fins de la réalisation d'écoutes téléphoniques peut être compatible avec la Convention (voir, par exemple, *Weber et Saravia c. Allemagne* (déc.), no 54934/00, § 115, CEDH 2006-XI, *Klass et autres*, § 51, et *Kennedy*, § 31, tous deux précités), à condition que cet organe soit suffisamment indépendant à l'égard de l'exécutif (*Dumitru Popescu c. Roumanie* (no 2), no 71525/01, § 71, 26 avril 2007). Par ailleurs, les procédures concernées doivent être examinées non seulement telles qu'elles existent en théorie, mais aussi telles qu'elles fonctionnent dans la pratique, pour autant cela puisse être vérifié sur la base de sources officielles fiables (*Ekimdzhiev et autres*, précité, § 307).

204. En l'espèce, la Cour note que la législation applicable prévoit des garanties destinées à assurer que la surveillance secrète ne soit utilisée qu'en cas de réelle nécessité. Premièrement, seul un nombre limité d'autorités peuvent demander une surveillance dans le cadre de leurs compétences respectives (paragraphe 33 ci-dessus). Deuxièmement, la loi prévoit une forme de contrôle interne préalable à l'introduction des demandes de surveillance, celles-ci devant émaner du chef de l'autorité d'application de la loi concernée et être préalablement approuvées par le

procureur compétent (pour un raisonnement similaire, voir, *Ekimdzhiev et autres*, précité, § 308). Troisièmement, la loi précise le contenu d'une demande d'autorisation de la surveillance et exige que celle-ci soit motivée (paragraphe 34 ci-dessus). Quatrièmement et surtout, la loi impose que le contrôle opérationnel soit préalablement autorisée par un juge. Exceptionnellement, en cas d'urgence, la police peut procéder à la surveillance sans cette autorisation, mais elle devra l'interrompre si elle n'obtient pas pareille autorisation dans les cinq jours suivant la mise en place de ladite mesure, et toute l'information réunie dans ce cadre devra alors être détruite. La Cour observe de surcroît que certains aspects pertinents de la procédure d'autorisation de la surveillance secrète ont fait l'objet d'un examen approfondi de la Cour constitutionnelle, laquelle a conclu, à cet égard, à l'absence d'éléments propres à jeter un doute sur le caractère effectif du contrôle de la surveillance secrète au stade de l'autorisation de la mesure en question (paragraphe 73 ci-dessus).

205. La Cour souscrit aux constats de la Cour constitutionnelle, dont il se dégage que l'exigence d'une autorisation juridictionnelle préalable de la surveillance secrète constitue une importante garantie de protection contre les abus de la part des services de l'État procédant à la surveillance en question. Cela étant, elle relève, par ailleurs, quelques éléments qui indiquent que le régime national d'autorisation de la surveillance secrète est incompatible avec la Convention.

206. La Cour rappelle avoir dit que le pouvoir de surveiller en secret les citoyens n'est tolérable, d'après la Convention, que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques, et que le service délivrant l'autorisation doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme des actes mettant en péril la sécurité nationale. Ledit service doit également s'assurer que l'interception requise satisfait au critère de « nécessité dans une société démocratique » prévu à l'article 8 § 2 de la Convention, notamment qu'elle est proportionnée aux buts légitimes poursuivis, en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs (*Klass et autres*, § 51, *Roman Zakharov*, § 260, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, no 62540/00, §§ 79-80, 28 juin 2007, et *Kennedy*, §§ 31-32, (précité). Elle considère que, dans les circonstances susdécrites, l'organe compétent, avant de délivrer l'autorisation de surveillance, doit vérifier l'existence « d'un soupçon raisonnable » à l'égard de la personne concernée et, en particulier, rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance. Or il ne ressort pas des éléments en sa possession que la législation applicable impose au juge statuant sur l'autorisation de surveillance de vérifier l'existence de ces éléments à l'égard de la personne visée : il s'agit-là, de l'avis de la Cour, d'une importante lacune de ladite législation.

207. La Cour observe que la législation incriminée par les requérants ne précise pas le contenu de l'autorisation d'interception ni n'impose au tribunal délivrant une telle autorisation de motiver sa décision, excepté dans le cas où celle-ci est défavorable à l'organe d'application de la loi qui souhaitait l'obtenir (voir, *idem*, § 259 et *Ekimdzhiev et autres*, § 309, tous deux précités, où les tribunaux délivrant une autorisation de recours à la surveillance secrète étaient tenus, à tout le moins en théorie, par l'obligation de motiver leurs décisions). Elle note, de plus, que la procédure

d'autorisation de la surveillance secrète est dépourvue de caractère contradictoire. Elle considère, sur ce point, que s'il est évident que la nature de la surveillance secrète commande que la procédure d'autorisation soit diligentée sans la participation de la personne qui en est la cible, la motivation de la décision statuant sur la demande d'autorisation est le seul moyen de s'assurer que le juge qui se prononce sur pareille demande a correctement examiné tant celle-ci que les documents produits à son appui, et qu'il s'est véritablement penché sur la question de savoir si la surveillance en question constituerait une ingérence justifiée et proportionnée dans l'exercice par la ou les personnes concernées, y compris toute personne susceptible d'être affectée de manière collatérale par cette surveillance, des droits protégés par l'article 8 de la Convention (*Ekimdzhiev et autres*, précité, § 313 et, *mutatis mutandis*, *Dragojević c. Croatie*, no 68995/11, §§ 91-92, 15 avril 2015). Elle estime que si le devoir d'établir la nécessité de l'interception incombe à l'organe demandeur, le juge qui examine une demande de surveillance secrète doit vérifier les motifs de cette mesure et n'accorder l'autorisation que s'il est convaincu que l'interception est légale, nécessaire et justifiée et, en plus, il doit en rendre compte dans les motifs de sa décision. Certes, l'absence de motivation ne peut pas automatiquement conduire à la conclusion que les juges qui délivrent les mandats de surveillance ont incorrectement apprécié les demandes qui leur étaient soumises à cette fin. La Cour a cependant égard au fait que la quasi-totalité des demandes d'autorisation de mise en place de la surveillance secrète sont portées devant le tribunal régional de Varsovie, que la plupart des agences réalisant la surveillance relèvent du ressort de cette juridiction, et que le nombre des demandes d'interception approuvées par les juges est élevé (paragraphe 84 ci-dessus). Elle considère que ces facteurs, considérés à l'aune des insuffisances exposées ci-dessus relativement à la procédure d'autorisation de mise en place de la surveillance secrète, sont de nature à conduire n'importe qui à douter de la capacité des juges à procéder en pratique à un contrôle judiciaire effectif de la surveillance en question (pour un raisonnement analogue, voir *Ekimdzhiev et autres*, précité, §§ 315-317).

208. La Cour note qu'en cas d'urgence, le procureur peut, dans un premier temps, autoriser le recours à des mesures d'interception sans l'approbation d'un juge, à condition que le tribunal donne ensuite son autorisation dans un délai de cinq jours. Elle observe que si aucune autorisation judiciaire n'est accordée, la surveillance doit cesser immédiatement et les matériaux collectés doivent être détruits. À cet égard, elle relève qu'en Pologne, l'application de la procédure d'autorisation d'urgence est justifiée seulement par le risque de perte des éléments de preuve, et non pas par la gravité ou la nature de l'infraction (voir, *a contrario*, *idem*, § 323, où le recours à la procédure d'urgence était limité aux cas de danger immédiat de commission d'une infraction grave ou de mise en péril de la sécurité nationale). Elle note que la législation applicable laisse aux autorités une grande latitude pour déterminer dans quelles situations il se justifie de recourir à la procédure d'urgence non judiciaire, ce qui engendre des risques de recours abusif à cette procédure et de détournement de l'obligation d'autorisation préalable. Elle estime que, compte tenu des dangers que le recours à pareille procédure d'urgence non judiciaire comporte pour la sphère privée de l'individu visé par la surveillance secrète, la législation applicable devrait comporter des garanties suffisantes pour en assurer une utilisation parcimonieuse et limitée aux cas dûment justifiés. De plus, même si en vertu de la loi la surveillance doit cesser dans un délai de cinq jours si aucune autorisation judiciaire n'est accordée, il n'est pas établi que la loi

applicable contient des garanties suffisantes contre l'utilisation répétitive de la mesure en question.

209. Pour ce qui est de la portée de l'examen effectué par le tribunal délivrant l'autorisation, la Cour observe qu'en Pologne, le tribunal qui statue sur l'autorisation de mise en place de la mesure de surveillance dispose uniquement du matériel que les services de l'État sollicitant une telle autorisation lui ont soumis à l'appui de leur demande. À cet égard, elle rappelle que le défaut de communication aux tribunaux de l'ensemble des informations pertinentes est susceptible d'ôter à ceux-ci le pouvoir de vérifier s'il existe une base factuelle suffisante à la mise en place des mesures de surveillance secrète (voir, *mutatis mutandis Ekhimdzhiev et autres*, précité, § 30). Elle rappelle en même temps avoir dit qu'il existe des techniques permettant de concilier, d'une part, les soucis légitimes de sécurité quant à la nature et aux sources de renseignement et, d'autre part, la nécessité d'accorder en suffisance au justiciable le bénéfice des règles de procédure (*Roman Zakharov*, précité, § 261). En l'espèce, elle observe que le tribunal qui statue sur l'autorisation de mise en place de la mesure de surveillance secrète a la possibilité de débouter l'organe demandeur de sa demande d'autorisation de recours à la mesure en question s'il estime que celle-ci est insuffisamment étayée. Elle note de plus qu'une décision prise en ce sens par le tribunal concerné ne prive pas l'organe en question de la possibilité de réintroduire sa demande après avoir vérifié lesquelles des informations en sa possession devraient ou pourraient être communiquées au juge de sorte qu'il puisse procéder à l'évaluation de la nécessité de la mise en place de la mesure de surveillance.

210. Eu égard aux considérations qui précèdent, la Cour considère que les procédures d'autorisation existant en droit polonais, telles qu'elles fonctionnent en pratique, sont inaptes à garantir que les mesures de surveillance secrète ne soient appliquées que lorsque cela est réellement justifié.

– *Procédures à suivre concernant la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées*

211. La Cour constate que le législateur polonais a prévu, dans chacune des lois réglementant la mise en place du contrôle opérationnel par divers services de police et de renseignement, un cadre pour la destruction des éléments recueillis au moyen dudit contrôle qui s'avèrent inutiles à la réalisation des buts que poursuivait le service de l'État concerné. Elle note que les différentes dispositions applicables en la matière énoncent des règles quasi analogues. Concernant, tout particulièrement, la loi sur la police, la Cour observe qu'aux termes des dispositions pertinentes, les éléments recueillis au moyen d'une surveillance secrète qui sont inutiles au regard de la finalité de celle-ci ou qui sont sans pertinence dans une procédure pénale doivent être détruits sans délai par une commission protocolaire. Elle relève qu'une obligation de destruction analogue est prévue relativement aux éléments collectés à l'issue du contrôle opérationnel mis en place dans les cas considérés comme urgents lorsque l'autorisation *a posteriori* de la surveillance en question n'est pas accordée. La Cour retient, en outre, que les éléments permettant l'engagement de poursuites pénales ou étant utiles à des poursuites en cours d'instruction sont transmis par les fonctionnaires compétents au procureur.

212. Il ressort par ailleurs des éléments en sa possession que la transmission des éléments recueillis par les services de l'État réalisant le contrôle opérationnel aux procureurs et aux tribunaux compétents s'effectue dans le respect des dispositions applicables aux informations classées. La Cour

note également que la législation applicable impose aux services de l'État procédant à la surveillance secrète de tenir des archives, sous une forme électronique, relativement aux documents concernant ladite surveillance.

213. La Cour considère que les dispositions relatives au traitement et à la destruction des informations interceptées au moyen d'un contrôle opérationnel énoncent des garanties de protection des données ainsi recueillies. Elle observe toutefois, d'une part, que la destruction des éléments collectés est confiée aux fonctionnaires des services de l'État réalisant la surveillance et, d'autre part, que l'application de la mesure en question n'est soumise à aucun contrôle externe et indépendant des services de l'État concernés (pour un raisonnement similaire, voir *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgari*e, précité, § 85, comparer aussi avec *Klass et autres*, précité, §§ 20 et 52, où un fonctionnaire possédant des qualifications requises pour accéder à la magistrature étudiait les renseignements réunis avant de transmettre aux services compétents ceux qui pouvaient être utilisés d'après la loi et procédait à la destruction de tous les autres documents éventuellement rassemblés).

– *Les dispositions relatives à la surveillance des communications couvertes par le secret professionnel*

214. La Cour note que le requérant Pietrzak a formulé des griefs relativement au caractère selon lui insuffisamment protecteur de la législation applicable à l'égard du secret professionnel des avocats.

215. À cet égard, elle rappelle que si l'article 8 protège la confidentialité de toute « correspondance » entre individus, il accorde une protection renforcée aux échanges entre les avocats et leurs clients. Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans toute société, à savoir la défense des justiciables. Or, un avocat ne peut mener à bien cette mission fondamentale s'il n'est pas à même de garantir à ceux dont il assure la défense que leurs échanges demeureront confidentiels (*mutatis mutandis Michaud c. France*, no 12323/11, § 118, CEDH 2012, et *R.E. c. Royaume-Uni*, no 62498/11, § 131, 27 octobre 2015).

216. Dans sa jurisprudence, la Cour a ainsi dégagé plusieurs garanties minimales qui devraient être énoncées dans la loi afin d'éviter les abus de pouvoir dans les cas où des éléments juridiquement protégés au titre du secret professionnel ont été collectés par le biais de mesures de surveillance secrète (*Dudchenko c. Russie,* no 37717/05, § 105, 7 novembre 2017).

217. Tout d'abord, la loi doit définir clairement le champ d'application du secret professionnel de l'avocat et préciser comment, dans quelles conditions et par qui la distinction doit être faite entre les documents protégés et ceux qui ne le sont pas. Étant donné que les relations confidentielles entre un avocat et ses clients appartiennent à un domaine particulièrement sensible qui concerne directement les droits de la défense, il est inacceptable que cette tâche soit confiée à un membre de l'exécutif, sans contrôle d'un juge indépendant (*Kopp c. Suisse*, 25 mars 1998, §§ 73 et 74, Recueil des arrêts et décisions 1998 II).

218. D'autre part, les dispositions concernant l'examen, l'utilisation et le stockage des éléments recueillis, les précautions à prendre lors de la communication de ceux-ci à d'autres parties et les circonstances dans lesquelles les enregistrements peuvent ou doivent être effacés ou

le matériel collecté détruit doivent fournir des garanties suffisantes à la protection des éléments couverts par le secret professionnel (*R.E.*, précité, §§ 138-39).

219. En l'espèce, la Cour relève que dans l'arrêt K 23/11 de la Cour constitutionnelle précité, la haute juridiction a conclu que la réglementation relative au contrôle opérationnel, dans sa formulation applicable à l'époque considérée, était contraire à la Constitution pour autant qu'elle ne prévoyait aucune garantie de protection de la confidentialité des échanges des dépositaires du secret professionnel. La Cour note que la Cour constitutionnelle a également estimé, d'une part, que la surveillance des communications entre les avocats et leurs clients n'était pas prohibée en soi et que pareille interdiction absolue de ce type n'était du reste pas souhaitable, et, d'autre part, qu'il était néanmoins impératif que la surveillance en question fût assortie de garanties adéquates de protection contre toute application abusive et toute collecte indue par les services de l'État procédant à la surveillance secrète des informations couvertes par le secret professionnel. Elle observe que, selon la haute juridiction, lesdites garanties devraient comporter au minimum un mécanisme de contrôle juridictionnel préventif des contenus potentiellement couverts par le secret professionnel de l'avocat qui soit apte à assurer la destruction des données devant rester confidentielles à ce titre.

220. La Cour note qu'à la différence de certaines des législations nationales examinées par elle par le passé (voir, par exemple, *Dudchenko*, précité, §§ 108-110), la législation polonaise relative à la surveillance secrète diligentée en amont ou en dehors d'une procédure pénale, dans sa rédaction actuellement applicable, prévoit des règles concernant le traitement des informations qui sont couvertes par le secret professionnel. Pour ce qui en particulier de la loi sur la police, la Cour se reporte à son article 19, lequel indique ce qui convient de faire de l'information relevant du privilège en question. Ainsi qu'il se dégage de la lettre de cette disposition législative, la Cour note que celle-ci opère une distinction entre, d'un côté, les informations qui bénéficient de la protection du secret professionnel absolu à laquelle ont droit les avocats de la défense et les prêtres et, d'un autre côté, les informations qui jouissent d'une protection moindre du secret en question, comme dans le cas des notaires, des avocats et des conseillers juridiques (sauf s'il s'agit d'un avocat de la défense), de conseillers fiscaux, de médecins, de médiateurs ou de journalistes.

221. La Cour note que les conditions matérielles dont dépend la possibilité pour les services de police de procéder à la surveillance secrète des communications entre les avocats et leurs clients sont les mêmes que celles qui s'appliquent à la surveillance secrète de l'ensemble des particuliers (pour un raisonnement similaire, voir *Dudchenko,* § 108 et *Ekimdzhiev et autres*, § 333, tous les deux précités). Elle observe que la législation applicable impose aux fonctionnaires de la police compétents de détruire les informations qui bénéficient de la protection du secret professionnel absolu. Elle relève, en même temps, que la législation en question n'interdit pas la surveillance secrète à l'endroit des avocats de la défense. Rappelant les constats, résumés ci-dessus, auxquels la Cour constitutionnelle est parvenue dans son arrêt K 23/11, la Cour observe que la Convention n'exige pas davantage des États contractants qu'ils proscrivent toute surveillance concernant les communications entre un détenu et son avocat. Elle souligne toutefois que la confidentialité de pareilles communications constitue un droit fondamental pour un individu et qu'elle touche directement aux droits de la défense. C'est pourquoi une dérogation à ce principe ne peut être autorisée que dans des cas exceptionnels et doit s'entourer de garanties adéquates contre les abus (voir, *mutatis mutandis*, *Erdem c. Allemagne*, no 38321/97, § 65, CEDH 2001 VII).

222. La Cour considère, par conséquent, qu'en principe, la surveillance des communications couvertes par le secret professionnel absolu ne devrait être permise que dans des situations exceptionnelles, comme par exemple dans le cas où il existe des indices fiables donnant à penser que l'avocat est complice d'un crime ou d'un délit particulièrement grave et que l'écoute de ses conversations avec son client constitue la seule méthode d'investigation possible dans l'enquête (à comparer avec l'arrêt *Erdem*, précité, § 62, l'affaire où les dérogations à la règle de confidentialité de la correspondance entre un détenu et son défenseur n'étaient autorisées que dans le contexte très précis de la lutte contre les infractions à caractère terroriste, *Mulders c. Pays-Bas* (déc.), no 23231/94, 6 avril 1995, où le recours à l'application des mesures de surveillance secrète à l'endroit des avocats était permis uniquement en cas d'urgence et lorsque l'avocat lui-même était soupçonné d'être complice des auteurs des infractions pour lesquelles la loi autorisait la mise en détention préventive, ou l'arrêt *R.E.*, précité, § 132, l'affaire dans laquelle l'obtention par la police d'informations couvertes par le secret professionnel des avocats était autorisée seulement en cas de menace pour la vie et l'intégrité physique des personnes ou la sécurité nationale et lorsque la surveillance était susceptible de procurer aux services de l'État compétents des renseignements nécessaires à la lutte contre lesdites menaces). Elle considère en outre qu'en pareilles circonstances, la surveillance des communications couvertes par le secret professionnel absolu devrait être soumise à l'autorisation préalable d'un organe extérieur et indépendant des services ayant recours à la surveillance en question, et de préférence d'un tribunal.

223. La Cour observe de plus qu'il résulte des dispositions de l'article 19 § 15 de la loi sur la police que la décision relative à ce qu'il convient de faire des informations collectées dans le cadre de mesures de surveillance secrète incombe en premier lieu au fonctionnaire de police compétent. Elle note, tout particulièrement, que celui-ci apprécie notamment si l'information ainsi recueillie est ou non couverte par le secret des communications entre un défenseur et son client et s'il convient par conséquent de la détruire sans délai, ou de la transmettre au tribunal compétent pour qu'il se prononce à son sujet dans les cas où l'information en question jouit d'une protection moindre du secret professionnel. À cet égard, la Cour rappelle avoir jugé que la décision quant au devenir des informations relevant du secret professionnel de l'avocat ne devrait pas, en principe, être laissée à la discrétion des services de l'État qui les ont recueillies mais devrait être confiée à un organe extérieur et indépendant des services de l'État intéressés, de préférence à un magistrat indépendant (pour un raisonnement similaire, voir *Kopp*, précité, § 73, où la détermination de ce qui relevait spécifiquement du mandat d'avocat et de ce qui avait trait à une activité n'étant pas celle d'un conseil revenait à un fonctionnaire spécialisé du service juridique d'un organisme appartenant à l'administration, sans aucun contrôle de la part d'un magistrat indépendant, et, *a contrario*, *Erdem*, précité, § 67, où le contrôle de l'application de la mesure de surveillance de la correspondance d'un détenu et de son avocat était assuré par un magistrat indépendant, qui ne devait avoir aucun lien avec l'instruction, et qui devait garder secret les informations dont il avait pris connaissance). La Cour relève que le Commissaire aux droits de l'homme de la République de Pologne a fait part de préoccupations analogues à ce propos, indiquant que si le mécanisme de sélection des contenus couverts par le secret professionnel de l'avocat pouvait déboucher sur la destruction des informations confidentielles, il n'empêchait pas

les services de l'État réalisant la surveillance secrète de prendre connaissance desdits contenus protégés (paragraphe 74 ci-dessus).

224. La Cour relève que les informations protégées qui jouissent d'une protection moindre du secret professionnel sont transmises au tribunal afin que celui-ci décide de ce qu'il convient d'en faire. Elle observe que les dispositions de l'article 19 § 15 de la loi sur la police imposent en outre au tribunal d'admettre ces éléments comme preuve si « cela est nécessaire dans la perspective du système judiciaire » et s'il n'existe aucun autre moyen d'établir les faits. La Cour constate à cet égard que la Commission de Venise, dans l'avis susmentionné, a estimé que les termes « nécessaire dans la perspective du système judiciaire » utilisés dans la législation en question étaient vagues à un point tel qu'ils rendaient possible une interprétation du secret professionnel vidant celui-ci de tout son sens. Elle observe qu'en conséquence de ses constats sur ce point, ladite instance a recommandé au législateur polonais d'envisager des règles plus strictes en la matière. La Cour a également égard au fait que le Commissaire aux droits de l'homme a fait part de ses préoccupations relativement à ces mêmes questions. Or, en l'espèce, le Gouvernement ne lui a fourni aucune indication quant à l'interprétation faite par les juridictions nationales du terme « nécessaire dans la perspective du système judiciaire ». La Cour rappelle avoir jugé que les dispositions relatives aux mesures de surveillance secrète potentiellement attentatoires au secret professionnel des avocats devraient satisfaire à des conditions particulièrement rigoureuses en matière de clarté et de précision pour pouvoir être considérées comme « une loi » (comparer avec *Erdem*, précité, § 67, où les dispositions régissant à la surveillance de la correspondance d'un détenu avec son avocat ont été jugées suffisamment claires et précises).

225. Dans ces circonstances, la Cour considère que les règles relatives à la protection du secret professionnel dans les opérations de surveillance secrète ne satisfont pas au critère de la prévisibilité de la loi.

– *Contrôle de l'application des mesures de surveillance secrète*

226. La Cour rappelle que l'appréciation de la question relative à l'existence en droit interne de garanties adéquates et effectives contre les éventuels abus de la part des autorités diligentant la surveillance est fonction, notamment, des instances compétentes pour contrôler celle-ci et des procédures de contrôle du déclenchement et de la mise en place desdites mesures restrictives (*Kennedy*, § 154, et *Roman Zakharov*, § 232, tous deux précités). De plus, ainsi qu'elle l'a déjà fait observer par le passé, le contrôle d'une mesure de surveillance secrète peut intervenir à trois stades : lorsqu'on l'ordonne, pendant qu'on la mène ou après qu'elle a cessé. Pour ce qui est des deux premières phases, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de la personne visée non seulement la surveillance en tant que telle, mais aussi le contrôle qui l'accompagne. Puisque l'on empêchera donc forcément l'intéressé d'introduire un recours effectif ou de prendre une part directe à un contrôle quelconque, il se révèle indispensable que les procédures existantes procurent en elles-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que la fonction de contrôle soit confiée à un juge, le contrôle par un organe non-judiciaire pouvant également passer pour compatible avec la

Convention dès lors que cet organe est indépendant des autorités qui procèdent à la surveillance et est investi de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent (*Klass et autres*, § 56 et *Roman Zakharov*, § 275, tous deux précités).

227. La Cour rappelle que dans l'affaire *Ekimdzhiev et autres* (précitée), elle a tenu compte des éléments ci-après dans l'examen de l'effectivité du mécanisme de contrôle à l'égard des autorités diligentant la surveillance secrète : a) l'indépendance de l'autorité de supervision, ses attributions et ses pouvoirs relativement aux infractions (le droit d'accéder à l'ensemble des matériaux et de prendre des mesures pour réparer les violations et, en particulier, d'ordonner la destruction des éléments interceptés de manière illégale) et b) l'ouverture des activités de l'organe de supervision à un droit de regard public (*ibidem*, § 334).

228. Concernant plus particulièrement l'exigence d'indépendance, la Cour a pris en compte, dans de précédentes affaires, le mode de désignation et le statut juridique des membres de l'organe de contrôle. En particulier, elle a jugé suffisamment indépendants les organes composés de députés -- de la majorité comme de l'opposition – ou de personnes possédant les qualifications requises pour accéder à la magistrature et nommées soit par le parlement, soit par le Premier ministre (voir, par exemple, *Klass et autres*, précité, §§ 21 et 56, *Weber et Saravia*, décision précitée, §§ 24-25 et 117, *Leander c. Suède*, 26 mars 1987, série A, no 116, *L. c. Norvège*, no 13564/88, décision de la Commission du 8 juin 1990, et *Kennedy*, précité, §§ 57 et 166). En revanche, elle a jugé insuffisamment indépendant un ministre de l'Intérieur qui non seulement était nommé par le pouvoir politique et membre de l'exécutif, mais de plus était directement impliqué dans la commande de moyens spéciaux de surveillance (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 85 et 87) ; elle a conclu dans le même sens pour ce qui est d'un procureur général et des procureurs de rang inférieur compétents (*Iordachi et autres c. Moldova*, no 25198/02, § 47, 10 février 2009 et *Roman Zakharov*, précité, §§ 279-284), et d'un organe spécifique dont les membres étaient censés superviser les demandes de surveillance spéciales émanant de l'agence qui les avait préalablement habilités et avaient été pour certains d'entre eux des anciens employés de l'agence en question (*Ekimdzhiev et autres*, précité, §§ 339-340).

229. Dans l'affaire *Klass et autres* (précitée), la Cour a également jugé compatible avec la Convention le système de contrôle de la surveillance constitué d'un fonctionnaire possédant les qualifications exigées pour accéder à la magistrature, qui assurait un premier contrôle au stade de l'exécution des mesures ordonnées, d'un comité parlementaire de contrôle composé de cinq membres du Parlement (dont les représentants de l'opposition), et enfin d'une commission indépendante qui statuait, d'office ou à la suite d'une plainte d'une personne se croyant surveillée, sur la légalité et la nécessité des mesures, lesquelles devaient être annulées par le ministre compétent si cette commission les déclarait illégales. La Cour rappelle en outre que dans l'affaire *Kennedy* (précitée), elle a approuvé un système de contrôle de la surveillance secrète dans lequel un organe indépendant, la Commission des pouvoirs d'enquête (Investigatory Powers Tribunal), formée de personnes qui occupaient ou avaient occupé de hautes fonctions judiciaires et de juristes chevronnés, était habilitée à annuler les mandats d'interception, travaillant avec le Commissaire chargé des interceptions (Interception of Communication Commissionner), un

fonctionnaire qui lui aussi occupait, ou avait occupé, de hautes fonctions dans la justice et avait accès à tous les mandats d'interception et demandes de tels mandats.

230. En l'espèce, le Gouvernement soutient que la mise en place du contrôle opérationnel était soumise à un contrôle juridictionnel *a priori* concernant son autorisation et son éventuelle prolongation subséquente et qu'en outre, les opérations des services de l'État réalisant la surveillance secrète faisaient l'objet d'une supervision de la part des procureurs compétents, de la chambre basse du Parlement (le « Sejm »), de la commission parlementaire chargée des services spéciaux et de la NIK.

231. Toutefois, la Cour observe qu'il ne ressort pas des éléments en sa possession que les juridictions polonaises soient compétentes pour exercer un contrôle suffisamment étendu sur les interceptions. Elle note à cet égard que le contrôle par les juridictions de la surveillance se limite au stade initial de l'autorisation (pour un raisonnement similaire, voir, *Roman Zakharov*, § 274, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, § 85 et *Ekimdzhiev et autres*, § 337, tous précités). Elle relève, tout particulièrement, que le tribunal qui accorde l'autorisation de surveillance n'est pas compétent pour en contrôler l'application, sauf dans le cas où il statue sur la prolongation d'un mandat d'interception ou sur une demande d'autorisation rétroactive d'une surveillance « urgente » mise en place sans autorisation préalable. Elle note, de surcroît, que le tribunal concerné n'est pas informé du résultat des interceptions, et qu'il n'a pas davantage le pouvoir de vérifier si les conditions auxquelles la décision d'octroyer l'autorisation était, le cas échéant, assortie ont été respectées.

232. Pour ce qui est des procureurs, la Cour note qu'ils sont impliqués à un certain degré dans le processus de contrôle préalable de la surveillance, qu'ils sont informés des résultats de l'interception et, en cas de demande faite par eux en ce sens, de son déroulement (paragraphes 33 et 38 ci-dessus). Elle accepte, par conséquent, qu'il existe un cadre légal ménageant, en théorie au moins, un certain contrôle des mesures de surveillance secrète par les procureurs.

233. En même temps, elle observe que, contrairement aux organes de contrôle évoqués ci-dessus au paragraphe 229, les procureurs en Pologne sont subordonnés au procureur en chef du parquet national, qui exerce en même temps les fonctions du ministre de la Justice (paragraphe 64 ci-dessus). Ce simple fait est de nature à compromettre leur capacité à exercer un contrôle indépendant à l'égard des services de l'État ayant recours aux mesures de surveillance secrète.

234. Pour ce qui est des pouvoirs et attributions des procureurs, la Cour constate que la portée du contrôle exercé par ceux-ci sur les opérations de surveillance secrète est limitée. En effet, bien que les procureurs supervisant les interceptions doivent être informés des résultats du contrôle opérationnel et puissent exiger des services procédant à celui-ci de leur soumettre tout document pertinent relativement à la surveillance en question, ils ne peuvent pour autant ordonner la destruction des éléments interceptés de manière illégale (voir, *a contrario*, *Kennedy*, précité, § 168, où tous les éléments interceptés devaient être détruits dès la découverte du caractère illégal d'une interception par le commissaire chargé des interceptions de communications).

235. Quant à la commission parlementaire supervisant les activités des services spéciaux, la Cour note que même si elle possède une vaste expertise en la matière, son rôle se limite, à l'égard des services de l'État réalisant la surveillance, à un contrôle général. La Cour observe en particulier que ladite commission parlementaire n'a aucun pouvoir de contrôle concernant l'application des

mesures d'interception dans des situations particulières, et qu'elle n'est pas davantage habilitée à prendre des mesures de redressement puisqu'elle ne peut ni annuler une autorisation d'interception, ni faire cesser une interception illégale, ni enfin ordonner la destruction des données recueillies de manière irrégulière (pour un raisonnement similaire, voir *Ekimdzhiev et autres*, précité, § 345). La Cour estime que ces considérations valent également concernant le contrôle exercé par le Sejm et la NIK à l'égard des services procédant à la surveillance. Sur ce point, elle partage en effet les conclusions de la Commission de Venise dans l'avis précité selon lesquelles le dispositif qui impose au ministre de l'Intérieur de soumettre chaque année au Parlement un rapport sur les surveillances menées par la police ne saurait remplacer un contrôle des opérations de surveillance spécifiques par un organe indépendant qui connaisse bien les pratiques de surveillance et d'interception et ne soit pas institutionnellement rattaché à la police, ni trop proche du pouvoir exécutif et des services de répression ou de renseignement. Elle considère qu'il en va de même pour ce qui est du rapport annuel établi par le chef du CBA et de celui élaboré par le chef du KAS à l'attention, respectivement, de la commission parlementaire supervisant les services spéciaux et du Sejm, lesquels rapports ne donnent qu'un aperçu général des activités de surveillance.

236. La Cour rappelle qu'il appartient au Gouvernement de démontrer, à l'aide d'exemples pertinents, l'effectivité concrète du système de contrôle (*Roman Zakharov*, précité, § 284). En l'espèce, elle constate que l'État défendeur est resté en défaut de prouver les affirmations avancées par lui selon lesquelles le contrôle exercé par les organismes susmentionnés à l'égard des services de l'État ayant recours aux mesures de surveillance secrète était effectif. Elle relève, à cet égard, que la Commission de Venise a recommandé à la Pologne de compléter le système d'autorisation juridictionnelle de la surveillance par d'autres garanties procédurales, préconisant un système de contrôle rétrospectif automatique de ces opérations par un organe qui serait indépendant de l'exécutif et des services de renseignement. La Cour considère, à l'instar de la Commission de Venise, qu'il serait souhaitable qu'en sus du contrôle juridictionnel à l'égard des opérations de surveillance, l'organe de contrôle indépendant soit habilité à contrôler régulièrement de sa propre initiative tous les aspects desdites opérations et, en particulier, à vérifier la légalité et la nécessité de la surveillance en question ainsi que le respect des limites fixées dans la décision d'autorisation. Elle estime de plus qu'un tel organe devrait avoir accès à toutes les informations qu'il jugerait nécessaires pour s'acquitter de son mandat et être pourvu des compétences requises pour détecter et faire cesser les abus.

237. La Cour estime qu'à la différence des systèmes de contrôle des opérations de surveillance secrète considérés ci-dessus au paragraphe 229, le dispositif qui est actuellement en place en Pologne ne garantit pas un contrôle effectif et indépendant à l'égard des services de l'État procédant à la surveillance en question. Eu égard aux insuffisances identifiées ci-dessus, elle est d'avis que, tel qu'il est organisé à l'heure actuelle, le mécanisme litigieux de contrôle de l'application des mesures de contrôle opérationnel n'est pas à même d'offrir des garanties adéquates contre les abus.

– *Notification de la surveillance de communications et recours disponibles*

238. La Cour va à présent se pencher sur la question de la notification de l'interception de communications, qui est indissolublement liée à celle de l'effectivité des recours judiciaires, et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance (*Roman Zakharov*, précité, § 234). Elle constate que l'article 19 § 16 de la loi sur la police énonce explicitement que les informations recueillies dans le cadre d'un contrôle opérationnel par les services de la police procédant à la surveillance secrète ne sont pas communiquées à la personne qui a fait l'objet de la surveillance en question. Il ressort en outre des éléments en sa possession qu'en Pologne, une personne qui a été soumise à une surveillance secrète n'en est pas informée, même après la cessation de celle-ci et même lorsque ladite surveillance n'a pas permis d'engager de poursuites à son endroit. Or, la Cour exige que l'individu placé sous surveillance en soit averti postérieurement, de sorte qu'il puisse être associé au contrôle de ladite mesure. Elle a ainsi énoncé une obligation générale de notification rétrospective, assortie de dérogations (*Roman Zakharov*, précité, § 288). En effet, bien qu'elle admette qu'il n'est, certes, pas possible en pratique d'exiger une notification dans tous les cas, elle considère qu'il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance et dès que la notification peut être donnée sans compromettre la finalité de la celles-ci (*Klass et autres*, précité, § 58, *Weber et Saravia*, décision précitée, § 135).

239. La Cour observe que, dans l'affaire *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev* (précitée), elle a estimé que l'absence d'obligation de donner notification de la surveillance, à un stade quelconque de celle-ci, à la personne visée par l'interception était incompatible avec la Convention, dès lors qu'elle ôtait à l'intéressé toute possibilité de demander réparation d'une atteinte illégale à ses droits tirés de l'article 8, et rendait les recours offerts par le droit interne théoriques et illusoires, et non pas concrets et effectifs. Elle a ainsi conclu que la législation en cause négligeait d'offrir une garantie importante contre l'utilisation indue de mesures spéciales de surveillance (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 90-91). La Cour est également parvenue à une conclusion analogue relativement à la législation russe concernant les interceptions des téléphones mobiles, les personnes dont les communications avaient été interceptées ne recevant à aucun moment, ni en aucune circonstance, notification de cette mesure, à moins qu'une procédure pénale fût déclenchée contre elles ou à moins d'une indiscrétion (*Roman Zakharov*, précité, § 289). Dans l'affaire *Kennedy*, au contraire, la Cour a considéré que l'absence d'obligation de notifier la mesure d'interception à un stade quelconque de l'application de celle-ci à la personne concernée était compatible avec la Convention, eu égard au fait qu'au Royaume-Uni toute personne soupçonnant que ses communications faisaient ou avaient fait l'objet d'interception pouvait saisir la commission des pouvoirs d'enquête, la compétence de celle-ci n'étant pas subordonnée à une notification de l'interception (*Kennedy*, précité, § 167).

240. La Cour observe que la législation polonaise régissant la surveillance secrète présente des similitudes avec les législations bulgare et russe susmentionnées, en ce qu'elle ne prévoit aucun mécanisme de notification de ladite surveillance – que ce soit à une personne soupçonnée d'implication dans des activités irrégulières ou à un individu indirectement visé par la mesure en question – à moins qu'une procédure pénale ne soit déclenchée contre la personne concernée et que les données interceptées aient servi d'éléments de preuve dans l'ouverture de cette procédure. Elle note qu'à deux occasions, la Cour constitutionnelle a attiré l'attention du législateur national sur ce qu'elle estimait être une lacune législative constitutive, en la matière, d'une violation des droits

énoncés à l'article 51 §§ 3 et 4 de la Constitution (garantissant le droit d'accès aux documents officiels et aux bases de données concernant l'individu et le droit d'exiger la rectification et l'élimination d'informations fausses, incomplètes ou recueillies de façon contraire à la loi). Il n'apparaît pas aux yeux de la Cour que le législateur polonais se soit conformé aux indications que lui a adressées sur ce point la Cour constitutionnelle, ni qu'une justification quelconque quant à ladite abstention du législateur ait été fournie par le Gouvernement. De plus, la Cour relève que la Commission de Venise, dans l'avis précité, a recommandé à la Pologne d'instaurer une obligation générale de notification rétrospective, assortie de dérogations, pour les services de l'État procédant à la surveillance.

241. La Cour note qu'en l'espèce, le Gouvernement défendeur estime que les requérants – comme toute personne qui se croit surveillée – auraient pu, sur le fondement de l'article 2 de la loi sur l'accès à l'information publique (paragraphe 59 ci-dessus), inviter le et/ou les responsables des services de police et de renseignement concernés à leur communiquer les informations supposément collectées à leur insu dans le cadre d'une mesure de surveillance secrète, et, en cas de décisions défavorables, attaquer celles-ci devant les tribunaux administratifs. La Cour n'est cependant pas convaincue par l'argument du Gouvernement concernant l'effectivité des recours en question. Elle observe, d'une part, que deux des requérants ont exercé, sans succès, le premier des recours indiqués par le Gouvernement, et, d'autre part, qu'une contestation des décisions des responsables des services de police et de renseignement en cause serait vraisemblablement vouée à l'échec eu égard à la jurisprudence constante de la Cour administrative suprême selon laquelle les informations relatives aux mesures opérationnelles d'investigation, aux méthodes employées, aux agents qui sont intervenus et aux données recueillies au moyen des mesures en question sont soumises à une protection analogue à celle des données classées et ne peuvent par conséquent être divulguées qu'aux seules personnes qui disposent d'une autorisation spécifique.

242. Pour ce qui est du recours constitutionnel que, selon le Gouvernement, les requérants auraient dû former dans le cas où les recours devant les autorités et tribunaux administratifs n'auraient pas prospéré, la Cour estime peu probable que pareil recours ait des chances d'aboutir dans le contexte en cause. Elle est d'avis qu'à supposer même que l'éventuel recours constitutionnel des requérants eût abouti à une déclaration d'inconstitutionnalité de la disposition citée par le Gouvernement, il n'aurait pas pour autant permis aux intéressés de faire contrôler la légalité d'une surveillance mise en place, le cas échéant, à leur endroit.

243. Enfin, pour autant que le Gouvernement invoque la possibilité pour les requérants d'engager une action en dommages et intérêts sur le fondement de l'article 4171 du code civil (paragraphe 68 ci-dessus), la Cour, prenant en considération les constats auxquels elle est parvenue ci-dessus relativement au recours constitutionnel, estime que les allégations du Gouvernement quant à ladite action, dont l'exercice dépendrait du succès préalable du recours constitutionnel en question, sont également spéculatives.

244. Quoi qu'il en soit, la Cour observe qu'en l'espèce le Gouvernement n'a pas démontré, par des exemples tirés de la jurisprudence interne, que l'exercice par les requérants des recours invoqués par lui aurait permis aux intéressés de faire établir l'éventuelle mise en place d'une surveillance les concernant, de faire contrôler la légalité de celle-ci et d'obtenir réparation en cas de surveillance illicite.

245. La Cour note par ailleurs que le Gouvernement ne mentionne pas d'autre recours qu'une personne souhaitant se plaindre de la surveillance secrète pourrait, selon lui, exercer, ce qui l'amène à conclure à l'absence de recours effectifs en la matière. Elle considère par conséquent qu'en privant l'individu visé par pareille mesure de la possibilité effective de contester celle-ci rétrospectivement, le droit national néglige d'offrir une importante garantie contre l'utilisation indue de la surveillance secrète.

– *Conclusion*

246. En conclusion, la Cour estime que le régime de contrôle opérationnel, tel qu'il est organisé à l'heure actuelle en Pologne, ne comporte pas de garanties adéquates et effectives contre l'arbitraire et le risque d'abus inhérent à tout système de surveillance. Elle est d'avis, tout particulièrement, que le champ d'application *ratione materiae* et *ratione personae* du dispositif relatif à la surveillance considérée n'est pas circonscrit avec une précision suffisante, que la durée totale d'application de ladite surveillance est discutable et que les règles relatives à une justification factuelle de celle-ci sont insuffisamment étoffées. Si le système de surveillance litigieux est, certes, assorti d'un mécanisme de contrôle juridictionnel *a priori*, la Cour n'est pas convaincue que la procédure d'autorisation, telle qu'elle est appliquée en pratique, soit à même de garantir qu'il n'y ait recours à la surveillance que lorsque cette mesure est « nécessaire dans une société démocratique ». À cet égard, elle observe, tout particulièrement, que la législation applicable n'impose pas au juge statuant sur l'autorisation de surveillance de vérifier l'existence « d'un soupçon raisonnable » à l'égard de la personne visée par la mesure en question et, en particulier, de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme des actes mettant en péril la sécurité nationale. Elle considère qu'il serait souhaitable que la procédure d'autorisation existante soit complétée par d'autres mécanismes procéduraux de contrôle *a posteriori*, tels que, lorsque la surveillance n'a pas débouché sur des poursuites pénales, une plainte ouverte aux personnes inquiètes d'une éventuelle surveillance les concernant, avec la possibilité d'une demande de contrôle juridictionnel et d'un contrôle effectué par un organisme indépendant. Elle observe qu'en l'état actuel, la loi ne semble pas contenir de dispositifs appropriés, et note que la loi n'impose pas non plus d'exigence de notification à la personne visée, même après un certain temps et même lorsque cela ne compromet pas la finalité de la mesure de surveillance. Elle considère enfin que la législation litigeuse ne protège pas non plus suffisamment les communications couvertes par le secret professionnel des avocats. L'ensemble des insuffisances susmentionnées font pencher la Cour en faveur du constat que le droit national ne prévoit pas de garanties suffisantes propres à prévenir tout recours excessif à la surveillance et les ingérences indues dans la vie privée des individus, garanties dont l'absence n'est pas suffisamment contrebalancée par l'actuel mécanisme de contrôle juridictionnel.

247. Pour les motifs exposés ci-dessus la Cour rejette l'exception de non-épuisement des voies de recours internes soulevée par le Gouvernement et conclut que le régime national de contrôle opérationnel, considéré dans son ensemble, ne répond pas aux exigences de l'article 8 de la Convention.

ii. La conservation des données de communication aux fins d'un accès éventuel par les autorités nationales compétentes

α) Principes généraux

248. La Cour a déjà indiqué que les données des abonnés aux services de télécommunications, les données relatives au trafic et les données de localisation, prises séparément ou combinées, peuvent concerner la vie privée des intéressés (*Ekimdzhiev et autres*, précité, § 372). Elle a jugé que le simple fait de conserver des données relatives à la vie privée d'un individu s'analyse en une ingérence au sens de l'article 8 (*Centrum för rättvisa*, précité, § 244). Elle a établi de plus que la conservation à l'insu de l'intéressé des données de ce type constituait de surcroît une ingérence dans l'exercice par la personne concernée du droit au respect de sa correspondance (*Ekimdzhiev et autres* précité, § 373, et *Ben Faiza c. France*, no 31446/12, §§ 66-67, 8 février 2018). Elle a observé en outre que l'utilisation ultérieure des informations mémorisées importait peu (*Amann c. Suisse* [GC], no 27798/95, § 69, CEDH 2000-II). Elle a enfin jugé que l'accès des autorités compétentes aux données ainsi conservées constituait une ingérence supplémentaire dans l'exercice par la personne concernée de ses droits protégés par l'article 8 (*Ekimdzhiev et autres*, § 376 et, *mutatis mutandis*, *Centrum för rättvisa*, § 244, tous deux précités).

249. La Cour rappelle qu'en conséquence de progrès technologiques intervenus au cours de deux dernières décennies dans le domaine des communications électroniques, pareilles communications peuvent dorénavant révéler un grand nombre d'informations personnelles. De plus, toute intrusion occasionnée par l'acquisition de données de communication associées est démultipliée par l'interception en masse, car ces données peuvent désormais faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts (*Centrum för rättvisa*, § 256, *Big Brother Watch et autres*, § 432, et *Ekimdzhiev et autres*, § 394, tous précités). L'acquisition des données de communication associées dans le cadre d'une interception en masse peut être tout aussi intrusive que l'acquisition du contenu des communications, en conséquence de quoi l'interception et la conservation des données de ce type, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, sans qu'il soit nécessaire que les dispositions juridiques régissant le traitement de ces données soient identiques en tous points à celles régissant le traitement du contenu des communications (*Big Brother Watch et autres*, §§ 363 et 416, *Centrum för rättvisa*, § 277, et *Ekimdzhiev et autres*, § 394, tous précités).

250. La Cour rappelle que, de la même manière, la conservation généralisée des données de communication par les fournisseurs de services de communication et leur traitement par les autorités dans des cas particuliers doivent s'accompagner, *mutatis mutandis*, des garanties et des garde-fous contre les abus similaires à ceux de la surveillance secrète (*Ekimdzhiev et autres*, précité, § 395).

251. En outre, dans l'arrêt *Roman Zakharov* précité, qui avait trait à d'autres buts légitimes tels que par exemple la protection de la sécurité nationale, la Cour a défini les garanties applicables en mettant l'accent sur les mécanismes de notification et les voies de recours prévues par le droit

national. Elle a fondé son appréciation de la conformité avec l'article 8 des mesures d'interception en cause sur les critères suivants : l'accessibilité du droit interne, la portée et la durée des mesures de surveillance secrète, les procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées, les procédures d'autorisation, les modalités de contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne (*ibidem*, § 238). Enfin, à l'occasion de l'examen d'affaires relatives aux régimes d'interception en masse de communications transfrontières et de réception de renseignements émanant de services de renseignement étrangers (*Big Brother Watch et autres* et *Centrum för rättvisa*, tous deux précités), la Cour a encore ajusté les critères susmentionnés, y compris l'exigence que le droit national définisse clairement les motifs pour lesquels l'interception de masse peut être autorisée, les circonstances dans lesquelles les communications d'un individu peuvent être interceptées et la procédure à suivre pour l'octroi de l'autorisation de la surveillance secrète.

β) L'application au cas d'espèce

252. En l'espèce, la Cour observe que les requérants dénoncent la législation nationale qui impose aux fournisseurs de services TIC de conserver les données qui sont traitées par eux relativement aux services de télécommunication qu'ils fournissent en vue d'un accès et d'un traitement éventuel par les services de police et de renseignement compétents.

253. À cet égard, elle relève que les données que les fournisseurs des services TIC sont tenus de conserver englobent des informations relatives notamment aux appels téléphoniques effectués ou reçus, aux numéros composés, à la durée des appels, à la localisation géographique des appareils mobiles, aux sites Internet consultés, aux connexions à des sites et aux adresses mail (paragraphe 46 ci-dessus). Elle renvoie à son observation ci-dessus (paragraphe 141) selon laquelle les données en question, dès lors qu'elles sont associées à l'expéditeur ou au destinataire d'une communication, permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts (voir, *mutatis mutandis, Ekimdzhiev et autres*, § 394, et *Big Brother Watch et autres*, § 342, tous deux précités). Dans ces circonstances, la Cour considère que la conservation des données en cause par les organismes habilités implique une intrusion dans la sphère privée des intéressés.

254. La Cour observe que la mesure litigeuse, bien qu'elle soit diligentée par des organismes privés – les fournisseurs de services de communication --, intervient en application d'une obligation découlant de la loi. Elle considère, par conséquent, que l'ingérence considérée est imputable aux autorités nationales (voir, *mutatis mutandis, Ekimdzhiev et autres*, précité, § 375).

255. La Cour renvoie à son observation ci-dessus (paragraphe 248) selon laquelle le simple fait de conserver des données relatives à la vie privée d'un individu s'analyse en une ingérence au sens de l'article 8. Elle rappelle en outre que l'accès des autorités nationales compétentes à de telles données constitue une ingérence supplémentaire dans ce droit fondamental. Il convient d'analyser ces deux mesures séparément, car chacune d'entre elles peut affecter les droits garantis par l'article 8 de la Convention de manière différente et à des degrés différents (voir, *mutatis mutandis, Centrum för rättvisa*, § 244, *Big Brother Watch et autres*, § 330, et *Ehimdzhiev et autres*, § 371, tous précités).

256. En l'espèce, la Cour observe qu'en application de l'article 20 c de la loi sur la police, qui constitue l'exemple *mutatis mutandis* d'une telle mesure pour les autres organismes, les fournisseurs des services TIC ont l'obligation de conserver les données qui sont traitées par eux relativement aux services qu'ils fournissent pendant une période d'une durée de douze mois de façon à les rendre accessibles aux services de police compétents à des fins de « prévention ou détection des activités criminelles, de sauvetage de vies humaines ou de protection de la santé, ou encore de réalisation d'opérations de recherche et de sauvetage ». Elle note que la loi sur la police ne précise pas quelles données peuvent être conservées mais renvoie à cet égard à d'autres textes relatifs aux télécommunications, à l'Internet et aux services postaux. Elle relève que le paragraphe 2 de l'article 180 c de la loi sur les télécommunications (paragraphe 60 ci-dessus) charge de surcroît les ministres compétents de fixer par voie de décrets la liste détaillée des données que les fournisseurs de services TIC doivent conserver en application de l'article 20 c de la loi sur la police. Elle note que la législation applicable a instauré un régime de surveillance dans le cadre duquel tout usager des services de télécommunications et d'Internet est concerné par la mesure de conservation des données associées à ses communications sans jamais en être informé. Elle observe que les cas dans lesquels la police et les services de renseignement peuvent accéder aux données qui ont ainsi été conservées sont libellés en des termes généraux, de sorte que les services de l'État en question peuvent accéder aux données en question et les traiter à toute fin utile à la réalisation de leurs attributions statutaires respectives. Elle note, par ailleurs, que le mécanisme de conservation litigieux des données de communication permet aux agents des services de l'État compétents d'accéder auxdites données directement, sans participation du personnel des prestataires de services TIC, dès lors qu'un tel accès est prévu dans une convention confidentielle passée entre la police et le prestataire. Elle relève qu'en conséquence d'une telle législation, les services de l'État intéressés ont en permanence et directement accès aux données de communication dans une mesure illimitée, sans même que les opérateurs de télécommunication le sachent et sans une quelconque intervention de leur part.

257. Dans ces circonstances, il est évident, aux yeux de la Cour, que l'ingérence découlant, dans l'exercice du droit des requérants au respect de leur vie privée, de l'obligation faite aux fournisseurs des services TIC de conserver les données associées à leurs communications, revêt un degré élevé de gravité. Elle note que la mesure en question peut à juste titre générer dans l'esprit des personnes concernées un sentiment de vulnérabilité et de surexposition au regard de tiers, et peut avoir des répercussions négatives sur la jouissance effective des droits fondamentaux qui leur sont reconnus, parmi lesquels le droit au respect de leur vie privée et de leur correspondance et le droit de nouer des relations avec autrui. À cet égard, la Cour se réfère à la jurisprudence de la CJUE présentée ci-dessus aux paragraphes 104 à 108, dont il se dégage que la haute juridiction européenne considère que les données relatives au trafic et à la localisation afférentes aux communication électroniques, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été collectées et que la conservation de telles données aux fins d'un accès éventuel par les autorités nationales compétentes comporte une ingérence « d'une vaste ampleur et d'une gravité particulière » dans l'exercice par les personnes concernées de leurs droits fondamentaux.

258. La Cour rappelle que dans l'affaire *Ekimdzhiev et autres* précitée (§§ 394-421), qui concernait un régime de conservation des données de communication similaire à celui qui est en cause en l'espèce, elle a examiné les garanties relatives à l'accès aux données collectées et à la conservation des données recueillies ; en revanche, elle ne s'est pas prononcée sur la conformité avec les exigences de l'article 8 du régime de conservation des données en question en tant que tel. Toutefois, elle note que les requérants en l'espèce se plaignent explicitement du régime de conservation des données de communication qui leur est applicable et de l'utilisation subséquente des données en question par les services de l'État ayant recours aux mesures de surveillance secrète (paragraphe 125 ci-dessus).

259. La Cour renvoie aux principes présentés aux paragraphes 248-251 ci-dessus, dont il se dégage que le droit national devrait, dans le cadre des garanties minimales et d'une manière adaptée à la forme particulière de surveillance dont il s'agit, définir le champ d'application de la mesure de surveillance en question et prévoir des procédures d'autorisation ou de réexamen appropriées en vue de la maintenir dans les limites de ce qui est nécessaire pour atteindre un ou plusieurs des buts légitimes envisagés par les autorités. En l'espèce, la Cour, statuant en considération de la gravité de l'ingérence considérée dans l'exercice par les requérants de leurs droits relevant de la sphère protégée par l'article 8 de la Convention, est d'avis que la mesure litigeuse devrait être entourée de garanties analogues. Elle estime que l'absence dans la législation applicable de dispositions ou de mécanismes capables d'adapter à ce qui est « nécessaire dans une société démocratique » l'étendue de l'ingérence incriminée dans l'exercice par les requérants de leurs droits protégés par l'article 8 de la Convention rend le régime de surveillance litigieux incompatible avec cette disposition conventionnelle.

260. La Cour observe que la législation incriminée par les requérants a suscité des réserves tant de la part de la Cour constitutionnelle que de la Commission de Venise quant au point de savoir si elle respecte les exigences de « clarté » et de « prévisibilité » d'une loi. Elle se réfère également à la jurisprudence de la CJUE présentée ci-dessus aux paragraphes 104 à 108, dont il ressort que la haute juridiction européenne considère que le système imposant une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques aux fins de lutte contre les infractions graves ne répond pas à l'exigence de proportionnalité. Elle observe que la jurisprudence subséquente de la CJUE (paragraphes 111-112 ci-dessus) précise que, même dans le contexte de la protection de la sécurité nationale, où la conservation des données de communication peut, sous certaines conditions, être ordonnée en tant que mesure généralisée et indifférenciée, l'application de la mesure en question ne devrait être autorisée que pour une période temporellement limitée au strict nécessaire et devrait faire l'objet d'un contrôle indépendant.

261. En l'espèce, il est évident, aux yeux de la Cour, que la législation mise en cause par les requérants impose une conservation généralisée et indifférenciée des données liées aux télécommunications, aux communications postales et aux communications numériques de l'ensemble des usagers des services de communications et qu'elle touche des personnes dont les données sont conservées même si elles ne se trouvent pas, même indirectement, dans une situation susceptible de donner lieu à de poursuites pénales. La Cour note que les données conservées de la sorte pendant une période de douze mois sont mises à disposition des services de police et de

renseignement compétents, qui peuvent y accéder et s'en servir à toute fin utile à la réalisation de leurs attributions statutaires respectives.

262. À cet égard, la Cour observe que, même si l'accès des services de l'État en question aux données mises à leur disposition par les prestataires de services TIC s'accompagne de quelques garanties de protection contre les éventuels abus, dont un mécanisme de contrôle judiciaire rétrospectif, lesdites garanties sont insuffisantes à remédier aux insuffisances relevées ci-dessus dans le régime de conservation des données de communication et ne peuvent, par conséquent, rendre le régime en question conforme aux exigences de l'article 8 de la Convention. La Cour se réfère à l'arrêt *SpaceNet et Telekom Deutschland* de la CJUE précité (paragraphe 115 ci-dessus), dans lequel la haute juridiction européenne a jugé que la conservation des données relatives au trafic et des données de localisation et l'accès à de telles données constituent des ingérences distinctes dans les droits fondamentaux des personnes concernées, nécessitant une justification distincte, et que, par conséquent, une législation nationale assurant le plein respect des conditions résultant de la jurisprudence en matière d'accès aux données conservées ne saurait, par nature, être susceptible ni de limiter ni même de remédier à l'ingérence grave dans les droits des personnes concernées qui résulterait de la conservation généralisée de données en question.

263. En l'espèce, la Cour observe que les requérants se plaignent également que la législation applicable, pour autant qu'elle prévoit un accès des services de police et de renseignement aux données conservées selon les modalités ci-dessus, est contraire à l'article 8 de la Convention. À cet égard, elle relève que lorsque la conservation des données de communication ne satisfait pas aux impératifs en matière de « qualité d'une loi » ni ne répond au principe de proportionnalité, si bien qu'elle est contraire à l'article 8, l'accès aux données en question, leur conservation ni leur traitement éventuels par les autorités ne peuvent eux non plus, pour la même raison, être conformes à l'article 8. La Cour se réfère à ce propos à l'arrêt *Commissioner of An Garda Síochána e.a.* de la CJUE précité (paragraphe 114 ci-dessus), dont il se dégage que la haute juridiction européenne a jugé que la conservation des données relatives au trafic et à la localisation afférentes aux communications électroniques ne pouvaient pas faire l'objet d'une conservation générale et indifférenciée aux fins de lutte contre la criminalité grave et que, par conséquent, l'accès aux données ne pouvait pas non plus être justifié par le même objectif. En l'espèce, la Cour n'aperçoit aucune raison qui puisse la conduire à s'écarter des conclusions de la CJUE sur ce point.

– *Conclusion*

264. Pour les raisons exposées ci-dessus, la Cour considère que la législation nationale, en application de laquelle les prestataires de services TIC sont tenus de conserver de manière généralisée et indifférenciée les données de communication aux fins d'un accès éventuel par les autorités nationales compétentes, s'avère insuffisante à limiter à ce qui est « nécessaire dans une société démocratique » l'ingérence dans l'exercice par les requérants du droit au respect de leur vie privée. Partant, elle conclut à la violation de l'article 8 de la Convention également en ce qui concerne la conservation des données de communication aux fins d'un accès éventuel par les autorités nationales compétentes.

iii. Le régime de surveillance secrète de la loi anti-terrorisme

265. La Cour note que le législateur polonais a adopté la loi anti-terrorisme aux fins de renforcer le dispositif national de lutte contre le terrorisme et de protection de la sécurité nationale. Elle constate qu'en vertu des dispositions pertinentes de la loi en question, les fonctionnaires de l'ABW sont autorisés à recourir à la surveillance secrète à l'endroit de ressortissants étrangers soupçonnés d'activités terroristes. Elle observe, en outre, que le catalogue des mesures de surveillance que lesdits fonctionnaires peuvent mettre en place à cette fin est précisé à l'article 9 de la même loi.

266. La Cour rappelle avoir dit que les sociétés démocratiques se trouvent menacées de nos jours par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. Elle admet, par conséquent, que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales (*Klass et autres*, précité, § 48).

267. La Cour souligne néanmoins que les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle réaffirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée. Ainsi, quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus (*idem*, § 50).

268. Se tournant vers les faits de l'espèce, la Cour observe que le champ d'application *ratione personae* de la loi anti-terrorisme, bien qu'il soit en principe limité aux seuls ressortissants étrangers, est en pratique plus large en ce qu'il permet aux fonctionnaires de l'ABW de surveiller indirectement les communications de tout individu qui est en contact avec les personnes visées, qu'il ait été placé lui-même ou non sous surveillance (*Ekimdzhiev et autres*, précité, § 263).

269. Elle note que les requérants soutiennent que le libellé des notions clés de la loi en question, desquelles dépend la possibilité pour les fonctionnaires de l'ABW de procéder à une surveillance secrète à l'endroit de ressortissants étrangers, à savoir les « activités terroristes », les « incidents à caractère terroriste » et les « individus soupçonnés d'activités terroristes », est large. À cet égard, la Cour rappelle avoir déjà dit, dans le contexte de l'affaire *Szabó et Vissy* précitée, qui est similaire à celui de la présente cause et concernait une législation sur les opérations secrètes de surveillance antiterroriste, que la nécessité d'éviter une rigidité excessive et de suivre l'évolution des circonstances fait que de nombreuses lois sont inévitablement formulées en termes plus ou moins vagues. Aussi, elle est convaincue que même dans le domaine de la surveillance secrète, où la prévisibilité revêt une importance particulière, les notions litigieuses apparaissent suffisamment claires pour satisfaire aux exigences de la légalité. En effet, aux yeux de la Cour, l'exigence de « prévisibilité » de la loi ne va pas jusqu'à obliger les États à adopter des dispositions légales énumérant en détail toutes les situations susceptibles d'entraîner la décision de lancer des opérations de surveillance secrète. La référence à des menaces terroristes ou à des opérations de sauvetage peut ainsi être considérée, en principe, comme donnant aux citoyens l'indication requise (*mutatis mutandis Szabó et Vissy*, précité, § 64).

270. Cependant, la Cour a également souligné que, s'agissant de questions touchant aux droits fondamentaux, la loi irait à l'encontre de la prééminence du droit, l'un des principes de base d'une société démocratique consacrés par la Convention, si le pouvoir d'appréciation accordé à l'exécutif en matière de sécurité nationale ne connaissait pas de limite. En conséquence, la législation doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante – compte tenu du but légitime poursuivi - pour fournir à l'individu une protection adéquate contre l'arbitraire (*Roman Zakharov*, § 247, et *Szabó et Vissy*, § 65, tous deux précités).

271. La Cour observe qu'en matière de surveillance secrète des ressortissants étrangers, l'article 9 paragraphe 1 de la loi anti-terrorisme met en place un régime *legis specialis* par rapport aux dispositions relatives à la surveillance secrète prévues par la loi sur la police, et qu'il permet aux fonctionnaires de l'ABW de surveiller en secret un ressortissant étranger pendant trois mois sans aucune autorisation judiciaire préalable. La Cour note en outre qu'il découle de la lettre des dispositions de l'article en question que le chef de l'ABW décide de la mise en place des mesures de surveillance, puis transmet sa décision motivée au ministre chargé de la supervision des services spéciaux de l'État et au procureur en chef du parquet national, lequel peut mettre fin à l'application desdites mesures.

272. La Cour rappelle avoir jugé que « les pouvoirs de surveillance secrète des citoyens (...) ne sont tolérables au regard de la Convention que dans la mesure où ils sont strictement nécessaires à la sauvegarde des institutions démocratiques » (*Klass et autres*, précité, § 42). Elle tient à souligner, sur ce point, que compte tenu du caractère particulier de l'ingérence en question et du potentiel des technologies de surveillance de pointe à porter atteinte à la vie privée des citoyens, une mesure de surveillance secrète ne peut être jugée conforme à la Convention que si elle est strictement nécessaire, à titre de considération générale, à la sauvegarde des institutions démocratiques et, à titre de considération particulière, à l'obtention de renseignements vitaux dans le cadre d'une opération individuelle. Selon la Cour, toute surveillance qui ne correspond pas à ces critères est susceptible d'être utilisée de manière abusive par les autorités, lesquelles disposent de technologies redoutables (*Szabó et Vissy*, précité, §§ 71-73).

273. En l'espèce, la Cour observe que l'application des mesures de surveillance secrète à l'égard des ressortissants étrangers par les fonctionnaires de l'ABW n'est soumise, pendant la période initiale de trois mois, à aucune autorisation ni aucun contrôle de la part d'une instance indépendante de ceux-ci, laquelle serait à même de limiter leur latitude dans la lecture des formules générales utilisées par la loi anti-terrorisme et de vérifier s'il existe dans chaque cas des raisons suffisantes d'intercepter les communications d'un particulier (voir, *mutatis mutandis*, *Roman Zakharov*, précité, § 249). De l'avis de la Cour, ce n'est que de cette manière-là que l'on peut satisfaire à la nécessité de garanties assurant que les mesures d'urgence sont utilisées avec parcimonie et uniquement dans des cas dûment justifiés (*idem*, précité, § 266).

274. Par ailleurs, la Cour constate, d'une part, que les fonctionnaires de l'ABW procèdent à la surveillance secrète sur la base de la décision du chef de l'ABW, dont ils relèvent de l'autorité et, d'autre part, que pareille décision du chef de l'ABW fait objet d'une supervision de la part du procureur en chef du parquet national et du ministre chargé des services spéciaux de l'État. Elle relève que l'intervention du juge est prévue seulement en cas de prolongation subséquente de l'application des mesures de surveillance à l'expiration de la période initiale de trois mois. Elle

note, par conséquent, que ni la mise en place de la surveillance secrète, ni l'application de celle-ci au cours de ladite période initiale ne sont soumises à aucun contrôle d'une instance indépendante et externe des fonctionnaires de l'ABW réalisant la surveillance en question.

275. La Cour a déjà indiqué par le passé que l'autorisation de mise en place des mesures de surveillance secrète par un organe non-judiciaire peut être compatible avec la Convention sous réserve que l'organe en question soit suffisamment indépendant du pouvoir exécutif. Elle rappelle en outre avoir jugé qu'eu égard aux menaces terroristes contemporaines, il peut y avoir des situations d'urgence dans lesquelles l'application obligatoire d'une autorisation judiciaire n'est pas réalisable, serait contre-productive en raison d'un manque de connaissances spécifiques ou reviendrait simplement à perdre un temps précieux (*Szabó et Vissy*, précité, § 80). Pareilles mesures doivent toutefois faire l'objet d'un contrôle *a posteriori*, qui est généralement requis dans les cas où la surveillance a été autorisée au préalable par une autorité non judiciaire *(idem*, § 81).

276. En l'espèce, la Cour considère que l'autorisation des mesures de surveillance secrète par le chef de l'ABW, auquel les fonctionnaires qui les réalisent sont subordonnés, et la supervision subséquente de l'application desdites mesures par un membre du pouvoir exécutif ayant des responsabilités politiques et un membre du parquet n'offrant pas de garanties d'indépendance adéquates vis-à-vis du pouvoir exécutif ne fournissent pas de garde-fous nécessaires contre les abus, ce d'autant que les personnes soumises à la surveillance n'en sont jamais informées et ne disposent d'aucun recours effectif qui leur permettrait de contester la légalité de la surveillance diligentée à leur endroit.

277. La Cour note, par ailleurs, qu'en vertu de l'article 9 § 8 de la loi anti-terrorisme, le procureur en chef du parquet national a le pouvoir d'ordonner la destruction des éléments non pertinents. Toutefois, dès lors que l'actuel procureur en chef du parquet national est en même temps ministre de la Justice, la Cour considère que l'impartialité et l'indépendance du procureur en chef du parquet national sont insuffisamment garanties.

Conclusion

278. Pour les raisons exposées ci-dessus, la Cour conclut que les dispositions relatives à la surveillance secrète de la loi anti-terrorisme ne satisfont pas non plus aux conditions de l'article 8 de la Convention.

279. Partant, elle conclut à la violation de cette disposition de la Convention.

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

280. Les requérants se plaignent de l'absence d'un recours effectif qui leur permettrait de faire valoir leur grief fondé sur l'article 8. Ils invoquent l'article 13 de la Convention, qui est ainsi libellé :

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

281. Compte tenu de la conclusion à laquelle elle est parvenue au sujet de l'article 8 de la Convention (paragraphes 246, 264 et 278-279 ci-dessus), la Cour estime qu'il n'y a pas lieu d'examiner séparément le grief soulevé sous l'angle de l'article 13, bien qu'il soit étroitement lié à

celui fondé sur l'article 8 et doive donc être déclaré recevable (*Liberty et autres*, § 73, et *Roman Zakharov*, § 307, tous deux précités).

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

282. Aux termes de l'article 41 de la Convention :

« Si la Cour déclare qu'il y a eu violation de la Convention ou de ses Protocoles, et si le droit interne de la Haute Partie contractante ne permet d'effacer qu'imparfaitement les conséquences de cette violation, la Cour accorde à la partie lésée, s'il y a lieu, une satisfaction équitable. »

A. Dommage

283. Les requérants ne demandent aucune réparation, estimant qu'un constat de violation constituerait en soi une réparation suffisante. Le Gouvernement ne s'y oppose pas. Partant, la Cour considère qu'il n'y a pas lieu d'octroyer aux requérants de somme pour dommage matériel ou moral.

B. Frais et dépens

284. Le requérant Mikołaj Pietrzak demande le remboursement des frais afférents à sa participation à l'audience du 26 septembre 2022 devant la Cour et à celle des requérants Wojciech Klicki et Barbara Grabowska-Moroz, ainsi qu'à celle de leur représentante, les ventilant comme suit : 2 166, 08 polish zlotys (PLN - 459,97 euros (EUR)) pour l'hébergement hôtelier des requérants Mikołaj Pietrzak, Wojciech Klicki et Barbara Grabowska-Moroz et celui de leur représentante, et 10 196, 99 PLN (2 142, 95 EUR) pour les billets d'avion des requérants Mikołaj Pietrzak et Wojciech Klicki et celui de leur représentante. La requérante Barbara Grabowska-Moroz réclame en outre le remboursement de 1 201, 85 PLN (252, 58 EUR) pour son billet d'avion. Enfin, la requérante Dominika Bychawska-Siniarska demande le remboursement de 2 479, 73 PLN (526, 48 EUR) relativement à l'hébergement hôtelier. Les requérants produisent des copies des factures pertinentes.

285. Le Gouvernement ne conteste pas les sommes demandées par les requérants, excepté celle que réclame la requérante Dominika Bychawska-Siniarska. À cet égard, il expose qu'il ressort du libellé de la facture d'hôtel soumise par celle-ci que l'hébergement hôtelier en question était censé accueillir trois personnes. Or, indique-t-il, seule la requérante a comparu à l'audience devant la Cour.

286. Selon la jurisprudence de la Cour, un requérant ne peut obtenir le remboursement de ses frais et dépens que dans la mesure où se trouvent établis leur réalité, leur nécessité et le caractère raisonnable de leur taux. En l'espèce, compte tenu des documents dont elle dispose et des critères exposés ci-dessus, la Cour alloue aux requérants Mikołaj Pietrzak, Barbara Grabowska-Moroz et Dominika Bychawska-Siniarska les sommes suivantes : 2 602, 92 EUR, 252, 58 EUR et 300 EUR au titre des frais et dépens relatifs à la procédure suivie devant elle et rejette le restant la demande formulée à ce titre par la requérante Dominika Bychawska-Siniarska.

PAR CES MOTIFS, LA COUR, À L'UNANIMITÉ,

1. *Décide* de joindre les requêtes ;
2. *Déclare* les requêtes recevables ;
3. *Dit* qu'il y a eu violation de l'article 8 de la Convention, concernant le grief relatif au régime de contrôle opérationnel;
4. *Dit* qu'il y a eu violation de l'article 8 de la Convention pour autant que le grief porte sur la conservation des données de communication aux fins d'un accès éventuel par les autorités nationales compétentes ;
5. *Dit* qu'il y a eu violation de l'article 8 de la Convention, concernant le grief relatif au régime de surveillance secrète de la loi anti-terrorisme ;
6. *Dit* qu'il n'y a pas lieu d'examiner le grief formulé sur le terrain de l'article 13 de la Convention ;

7. *Dit*

a) que l'État défendeur doit verser, dans les trois mois à compter de la date à laquelle l'arrêt sera devenu définitif conformément à l'article 44 § 2 de la Convention, les sommes suivantes, à convertir dans la monnaie de l'État défendeur, au taux applicable à la date du règlement :

   i. 2 602, 92 EUR au requérant Mikołaj Pietrzak, plus tout montant pouvant être dû par ce requérant à titre d'impôt, pour frais et dépens ;
   ii. 252, 58 EUR à la requérante Barbara Grabowska-Moroz, plus tout montant pouvant être dû par cette requérante à titre d'impôt, pour frais et dépens ;
   iii. 300 EUR à la requérante Dominika Bychawska-Siniarska, plus tout montant pouvant être dû par cette requérante à titre d'impôt, pour frais et dépens ;

b) qu'à compter de l'expiration dudit délai et jusqu'au versement, ces montants seront à majorer d'un intérêt simple à un taux égal à celui de la facilité de prêt marginal de la Banque centrale européenne applicable pendant cette période, augmenté de trois points de pourcentage ;

8. *Rejette*, à l'unanimité, la demande de satisfaction équitable pour le surplus.

Fait en français, puis prononcé en audience publique à Strasbourg, au Palais des droits de l'homme le 28 mai 2024.

Ilse Freiwirth
Greffière

Marko Bošnjak
Président

ANNEXE 1

Liste des requérants : OMISSIS

ANNEXE 2

LES DISPOSITIONS PERTINENTES DE LA LÉGISLATION PORTANT RÉGLEMENTATION DES SERVICES DE L'ÉTAT AYANT RECOURS À LA SURVEILLANCE SECRÈTE[42]

I. LA LOI DU 6 AVRIL 1990 SUR LA POLICE

Article 19

« 1. À l'occasion de l'application par la police de mesures opérationnelles d'investigation aux fins de la prévention et de la découverte [des infractions mentionnées ci-après], de la découverte de [leurs] auteurs ou de la collecte et de l'enregistrement des éléments de preuve concernant les infractions :

1) contre la vie qui sont réprimées par les articles 148-150 du code pénal (homicide, infanticide, euthanasie) ;

2) qui sont réprimées par les articles 134 (attentat contre le président de la République), 135 § 1 (voies de fait ou outrage au président), 136 § 1 (voies de fait ou outrage à un chef d'État étranger), 156 §§ 1 et 3 (lésions corporelles graves), (...) 163 §§ 1 et 3 (mise en danger de la vie d'autrui), 164 § 1 (mise en danger immédiate), 165 §§ 1 et 3 (autres mises en danger), 166 (piratage), 167 (formation d'un danger à bord d'un navire ou d'un aéronef ou [détention] de substances dangereuses), 173 §§ 1 et 3 ([provocation d'une] catastrophe sur terre, sur l'eau ou concernant le trafic aérien), 189 (détention illégale), 189a (traite des êtres humains), (...) 211a (adoption illégale), 223 (voies de fait), (...) 228 §§ 1 et 3-5 (corruption passive), 229 §§ 1 et 3-5 (corruption active), 230 § 1 (trafic d'influence), 230a § 1 et 231 § 2 (trafic d'influence - clause d'inviolabilité), 232 (violence et menace illégales à l'encontre d'une cour ou d'un tribunal internationaux), 233 §§ 1, 1a, 4 et 6 (faux témoignage), 234 (fausse accusation), 235 (contrefaçon de preuve à charge), 236 § 1 (contrefaçon de preuve d'innocence), 238 (fausses allégations d'infraction), 239 § 1 (assistance à un délinquant et complicité), 240 § 1 (non-dénonciation d'une infraction), 245 (subornation de témoins), 246 (coercition illégale en vue de l'obtention d'une déclaration), 252 §§ 1-3 (prise d'otage), 258 (association de malfaiteurs), (...) 269 (sabotage informatique), (...) 270a §§ 1 et 2 (faux), 271a § 1 et 2 (fausse facture), 277a § 1 (fausse facture [pour un montant] supérieur à 10 millions de zlotys), (...) 280-282 (vol à main armée, vol aggravé, extorsion), 285 § 1 (raccordement frauduleux à une ligne téléphonique [appartenant à] autrui), 286 § 1 (fraude), (...) 296 §§ 1-3 (abus de confiance), 296a §§ 1-2 et 4 (corruption de dirigeants), 299 §§ 1-6 (blanchiment d'argent) et 310 §§ 1, 2 et 4 (contrefaçon) du code pénal ;

2a) qui sont réprimées par les articles 46 §§ 1-2 et 4 (acceptation ou fourniture d'avantages financiers ou personnels en relation avec des compétitions sportives), 47 (participation à des paris mutuels concernant des événements sportifs [en ayant] connaissance [de l'existence] d'un acte criminel indiqué à l'article 46), et 48 §§ 1-2 (rémunération de la fixation d'un résultat spécifique ou du déroulement d'un événement sportif) de la loi du 25 juin 2010 sur le sport ;

2b) qui sont réprimées par les articles 178-183 de la loi du 29 juillet 2005 sur les marchés d'instruments financiers (...) les articles 99-100 de la loi du 29 juillet 2005 sur l'offre publique et les conditions d'introduction d'instruments financiers sur le marché organisé et dans les sociétés publiques (...) ;

3) contre l'économie qui sont réprimées par les articles 296-306 du code pénal et qui ont occasionné un préjudice d'une valeur [au moins] cinquante fois supérieure à celle du salaire minimum (...) (délits d'abus de confiance, de corruption de dirigeants, de corruption active et passive dans le secteur privé, de fraude financière, au crédit et aux subventions, de fraude à l'assurance, de blanchiment d'argent, de privation illégale de la capacité d'un créancier à faire valoir les biens d'un débiteur, de faillite apparente, d'actes [commis] au détriment d'un créancier, [à savoir] défaut ou limitation d'exécution d'obligations envers des créanciers par la création d'une nouvelle unité commerciale, par faillite intentionnelle, faillite par imprudence, favorisation de créanciers ou corruption économique de créanciers, de dommages matériels causés à une personne physique ou morale ou à une unité organisationnelle ne disposant d'aucune personnalité juridique en ne tenant pas de registres des activités commerciales ou en les menant de manière peu fiable ou mensongère, d'utilisation abusive de la procédure d'appel d'offres public ou d'obstruction à celle-ci, de falsification du marquage des produits) ;

3a) contre la liberté et la pudeur, si la victime est un mineur ou si le contenu pornographique, visé à l'article 202 du code pénal implique un mineur ;

3b) visées au chapitre 11 de la loi du 23 juillet 2003 sur la protection des monuments, au chapitre 5 de la loi du 14 juillet 1983 sur les ressources archivistiques nationales et les archives, au chapitre 5a de la loi du 21 novembre 1996 sur les musées, au chapitre 11a de la loi du 27 juin 1997 sur les bibliothèques et au chapitre 6 de la loi du 25 mai 2017 sur la restitution des biens culturels nationaux ;

4) à la loi fiscale, si la valeur de l'objet de l'infraction ou celle du dommage occasionné aux fonds publics est [au moins] cinquante fois supérieure à la valeur du salaire minimum ;

4a) qui sont réprimées par l'article 107 § 1 du code pénal fiscal ;

5) la fabrication, la détention ou le commerce illégal d'armes, de munitions, d'explosifs, de substances toxiques, de substances psychotropes et de leurs précurseurs, ainsi que de matières nucléaires et radioactives ;

6) listées à l'article 8 de la loi introductive au code pénal du 6 juin 1997 ;

7) listées aux articles 43-46 de la loi du 1er juillet 2005 relative à la collecte, au stockage et à la transplantation de cellules, tissus et organes,

8) qui sont réprimées tant en vertu de la législation répressive polonaise que des accords et des traités internationaux ;

9) listées aux points 1-8 ci-dessus, à l'article 45 § 2 du code pénal et à l'article 33 § 2 du code pénal fiscal (...) ;

- dès lors que d'autres moyens paraissent inefficaces ou inutiles, le tribunal, statuant sur une demande écrite formée par le chef de la police nationale, le chef de la police régionale ou le chef du bureau d'investigations de police nationale et préalablement approuvée par le procureur compétent (le procureur en chef du parquet national ou le procureur régional) peut ordonner un contrôle opérationnel.

1a. La demande mentionnée au paragraphe 1 doit être étayée par des éléments justifiant la mise en place du contrôle opérationnel.

2. La décision visée au paragraphe 1 est rendue par le tribunal régional du siège de l'unité demanderesse de la police nationale.

3. En cas d'urgence et, tout particulièrement, de risque de perte d'informations ou d'altération des éléments de preuve, le chef de la police nationale, le chef du Bureau central d'investigation ou le chef de la police régionale peut ordonner un contrôle opérationnel sous réserve de l'obtention d'une autorisation préalable écrite du procureur compétent visé au paragraphe 1. Il soumet en même temps au tribunal régional compétent une demande d'autorisation de mise en place du contrôle opérationnel. Si l'autorisation n'est pas obtenue dans les cinq jours, le contrôle opérationnel est interrompu et les informations recueillies au moyen dudit contrôle durant ce délai sont détruites par une commission protocolaire.

(...)

5. En cas de besoin de recourir à un contrôle opérationnel à l'endroit d'un suspect ou d'un accusé, la demande de l'organe de police compétent mentionnée au paragraphe 1 doit comporter les informations relatives à la procédure diligentée contre la personne visée.

6. Le contrôle opérationnel est réalisé en secret au moyen des mesures suivantes :

1) l'interception et l'enregistrement du contenu de conversations téléphoniques ou de celles empruntant les réseaux de télécommunications ;

2) la collecte et l'enregistrement d'images ou de messages sonores dans des locaux, des moyens de transport ou des lieux autres que des lieux publics ;

3) l'interception et l'enregistrement du contenu de correspondances, y compris de la correspondance numérique ;

4) la collecte et l'enregistrement de données figurant sur des supports informatiques, des équipements terminaux de télécommunications ou des systèmes informatiques et téléinformatiques ;

5) la saisie de courriers postaux et le contrôle de leur contenu.

6a. L'enregistrement dans les endroits indiqués à l'article 15 alinéa 1 point 4a des images dont il est question au paragraphe 6 point 2 ne relève pas du contrôle opérationnel.

6b. La mise en œuvre de la mesure mentionnée à l'alinéa 6a ne nécessite pas d'autorisation juridictionnelle.

7. La demande d'autorisation de mise en place d'un contrôle opérationnel mentionnée à l'alinéa 1 doit indiquer notamment :

1) le numéro du dossier ou son cryptonyme,

2) les éléments factuels se rapportant à une infraction avec, si possible, leur qualification juridique,

3) les circonstances justifiant le recours à un contrôle opérationnel, y compris celles montrant que d'autres moyens seraient inefficaces ou inadéquats,

4) les éléments permettant de clairement identifier l'objet du contrôle opérationnel ainsi que l'endroit où il aura lieu et les moyens avec lesquels il sera réalisé,

5) l'objectif, la date et le type de contrôle opérationnel dont il s'agit.

8. Le contrôle opérationnel est autorisé pour une période n'excédant pas trois mois. Le tribunal régional peut (...), à la demande de l'organe de la police compétent et sur autorisation écrite du procureur, ordonner une prolongation pour une période supplémentaire n'excédant pas trois mois si les motifs initiaux de la mise en place du contrôle opérationnel sont encore valables.

9. Dans les cas dument justifiés, si la survenance de faits nouveaux au cours du contrôle opérationnel impose qu'il soit procédé à la prévention ou à la détection d'une activité criminelle, à la recherche de personnes se livrant à pareille activité ou à la collecte d'éléments de preuve, le tribunal régional, statuant sur une demande écrite formée par le chef de la police nationale et préalablement approuvée par écrit par le procureur en chef du parquet national, peut prolonger la mise en place du contrôle opérationnel pendant plusieurs périodes consécutives pour une durée maximale globale de 12 mois.

9a. Le chef de la police nationale, le chef du Bureau central d'investigation et le chef de la police régionale peuvent autoriser leurs adjoints respectifs à formuler les demandes indiquées aux alinéas 1, 3, 8 et 9, ou à ordonner la réalisation d'un contrôle opérationnel selon les modalités qui sont précisées à l'alinéa 3.

10. Les dispositions des alinéas 1a et 7 s'appliquent *mutatis mutandis* aux demandes mentionnées respectivement aux alinéas 3, 8 et 9. Le tribunal statuant sur les demandes relatives aux décisions visées aux alinéas 1, 3, 8 et 9 examine les éléments présentés à l'appui de celles-ci, y compris ceux déjà recueillis dans le cadre du contrôle opérationnel.

11. Le tribunal régional qui examine les demandes mentionnées aux alinéas 1, 3-5, 8 et 9 statue à juge unique. Celui-ci accomplit les différents actes de procédure dans des conditions [analogues à celles qui sont] prévues pour le transfert, la conservation et la divulgation d'informations classifiées et en prenant en compte de manière appropriée les dispositions émises sur le fondement de l'article 181 § 2 du code de procédure pénale. Seuls le procureur et le représentant de l'autorité demanderesse participent à la séance du tribunal.

12. Les sociétés de télécommunications, les opérateurs postaux et les prestataires de services fournis par voie électronique ont l'obligation d'assurer, à leurs frais, les conditions techniques et organisationnelles rendant possible la mise en œuvre du contrôle opérationnel par la police.

12a. Les prestataires de services fournis par voie électronique qui sont des micro-entrepreneurs au sens de la loi du 2 juillet 2004 sur la liberté d'activité économique assurent les conditions techniques et organisationnelles rendant possible la réalisation du contrôle opérationnel par la police au moyen de leur infrastructure.

13. Le contrôle opérationnel doit prendre fin dès que les raisons qui ont justifié sa mise en place ont cessé d'exister et au plus tard à l'expiration de la période pour laquelle il a été autorisé.

14. L'autorité de police visée à l'alinéa 1 informe le procureur compétent des éléments qui sont ressortis du contrôle opérationnel et, en cas de demande faite en ces sens par ledit procureur, de la manière dont le contrôle a été conduit.

15. En cas d'obtention d'éléments de preuve permettant l'engagement d'une procédure pénale ou s'avérant pertinents à l'égard de poursuites pénales en cours, le chef de la police nationale, le chef du Bureau central d'investigation ou le chef de la police départementale transmet au procureur compétent l'ensemble des éléments qui ont été recueillis au moyen du contrôle opérationnel, si nécessaire avec une demande d'ouverture d'une procédure pénale. Les dispositions de l'article 393 § 1 alinéa phrase 1 du code de procédure pénale s'appliquent *mutatis mutandis* à la procédure menée par le tribunal relativement à ces éléments.

(...)

15f. Lorsque les éléments visés à l'article 19 alinéa 15 de la loi sur la police :

1) contiennent les informations visées à l'article 178 du code de procédure pénale, le chef de la police nationale, le chef du Bureau central d'investigation ou le chef de la police départementale ordonne leur destruction immédiate par une commission protocolaire ;

2) sont susceptibles de contenir des informations visées à l'article 178a ou à l'article 180 § 3 du code de procédure pénale, à l'exception des informations relatives aux infractions mentionnées à l'article 240 § 1 du code pénal et de celles couvertes par le secret lié à l'exercice des professions ou des fonctions visées à l'article 180 § 2 du code de procédure pénale, le chef de la police, le chef du Bureau central d'investigation ou le chef de la police départementale transmet lesdits éléments au procureur.

15g. Dans le cas prévu à l'alinéa 15f point 2, le procureur transmet les éléments en question au tribunal qui a autorisé la mise en place du contrôle opérationnel ou a donné son accord conformément aux dispositions de l'alinéa 3, et l'invite :

1) à préciser lesquelles des informations transmises relèvent de l'alinéa 15f point 2 ;

2) à autoriser l'utilisation dans une procédure pénale des informations couvertes par le secret relatif aux professions visées à l'article 180 § 2 du code de procédure pénale, lesquelles ne relèvent pas des interdictions énoncées aux articles 178a et 180 § 3 du même code, à l'exception de celles qui concernent les infractions réprimées par l'article 240 § 1 du code pénal.

15h. Le tribunal statue sans délai sur la requête du procureur et peut autoriser l'utilisation dans une procédure pénale des informations visées à l'alinéa 15g point 2 s'il estime que l'intérêt de la bonne administration de la justice l'exige et qu'un fait pertinent ne peut pas être établi au moyen d'une autre preuve, ou, dans le cas contraire, ordonner leur destruction.

15i. Le procureur dispose d'un droit de recours à l'égard de la décision du tribunal refusant l'autorisation de l'utilisation dans une procédure pénale des informations visées à l'alinéa 15g point 2. Les dispositions du code de procédure pénale s'appliquent *mutatis mutandis* audit recours du procureur.

15j. L'autorité de police est tenue de se conformer à l'ordre de destruction du tribunal concernant les éléments visés à l'alinéa 15h et doit ordonner leur destruction sans délai par une commission protocolaire. Elle informe en outre immédiatement le procureur indiqué à l'alinéa 15g de la destruction des éléments en question.

16. La personne visée par le contrôle opérationnel n'a pas accès aux éléments recueillis au cours de celui-ci. Cette disposition ne la prive pas des droits qui sont énoncés à l'article 321 du code de procédure pénale.

16a. Le tribunal régional, le procureur en chef du parquet national, le procureur régional et l'autorité de police [compétente] tiennent des registres des décisions, (...) des autorisations écrites, des demandes et des ordres relatifs au contrôle opérationnel.

16b. Le chef de la police nationale tient un registre central des demandes et des ordres concernant les contrôles opérationnels réalisés par les fonctionnaires de la police nationale (...)

16c. Les unités de la police procédant aux contrôles opérationnels peuvent tenir des registres des informations figurant dans [l'ensemble de] la documentation relative au contrôle opérationnel (...)

16d. Les registres indiqués aux alinéas 16a-16c sont établis sous forme électronique dans le respect des dispositions relatives à la protection des informations classées.

(...)

17. Les éléments recueillis dans le cadre d'un contrôle opérationnel qui ne constituent pas des moyens de preuve permettant l'engagement de poursuites pénales ou qui sont inutiles à une procédure pénale en cours d'instruction font l'objet d'une destruction immédiate par une commission protocolaire. La destruction de ces éléments est ordonnée par l'autorité de police qui a sollicité l'autorisation de mise en place du contrôle opérationnel.

17a. L'autorité de police en question informe sans délai le procureur indiqué à l'alinéa 1 de la destruction de ces éléments.

(...) »

Article 20c

« 1. Afin de prévenir ou identifier des infractions pénales ou fiscales, de sauver des vies humaines ou de protéger la santé humaine, ou encore de réaliser des opérations de recherche ou de sauvetage, la police peut conserver les données qui ne livrent pas le contenu des télécommunications, des communications postales et des communications numériques qui sont précisées :

1) aux articles 180c et 180d de la loi du 16 juillet 2004 sur les télécommunications (...),

2) à l'article 82 alinéa. 1 point 1 de la loi du 23 novembre 2012 sur la poste (...),

3) à l'article 18 alinéas 1-, de la loi du 18 juillet 2002 sur la fourniture de services par voie numérique (...)

- et peut les traiter à l'insu et sans le consentement de la personne visée.

2. L'entreprise de télécommunications, l'opérateur postal ou le prestataire de services fournis par voie numérique sont tenus de mettre ces données à disposition :

1) du fonctionnaire de police indiqué dans la demande écrite du chef de la police, du chef du Bureau central d'investigation, du chef de la police départemental ou d'une personne mandatée par eux;

2) du fonctionnaire de police disposant d'une autorisation écrite d'une autorité mentionnée à l'alinéa 1 - sur sa demande formulée oralement ;

3) du fonctionnaire de police disposant d'une autorisation écrite d'une autorité visée à l'alinéa 1 - par l'intermédiaire d'un réseau de télécommunications.

3. Dans le cas indiqué au paragraphe 2 alinéa 3, la mise à disposition des données visées à l'alinéa 1 s'effectue sans la participation des employés de l'entreprise de télécommunications,

de l'opérateur postal ou du prestataire de services fournissant des services par voie électronique, ou avec la participation nécessaire de ceux-ci lorsqu'une telle possibilité est prévue dans un accord passé entre le commandant en chef de la police nationale et cette entité.

4. La communication à la police des données visées au paragraphe 1 peut se faire par le biais du réseau de télécommunications si :

1) les réseaux de télécommunications utilisés offrent :

a) la possibilité de déterminer la personne qui a obtenu lesdites données, le type de données en question et le moment où elles ont été recueillies,

b) une sécurité technique et organisationnelle suffisante pour empêcher une personne non autorisée d'accéder aux données ;

2) [pareille communication] est justifiée par la spécificité ou l'étendue des activités des unités organisationnelles de la police ou des missions accomplies par celles-ci.

5. Le commandant en chef de la police nationale, le commandant du Bureau central d'investigation et le commandant régional de la police tiennent des registres des demandes d'accès aux données liées aux télécommunications, aux communications postales et aux communications numériques, dans lesquels sont consignées les informations identifiant l'unité demanderesse, le fonctionnaire demandeur de la police nationale et le fonctionnaire de la police nationale qui a recueilli les données en question, le type de données recueillies, leur finalité et le moment où elles ont été obtenues. Les registres en question sont tenus sous un format numérique, à moins que les dispositions relatives à la protection des informations classées n'en disposent autrement.

6. Les données visées au paragraphe 1 qui sont utiles à une procédure pénale sont transmises par le commandant en chef de la police nationale, le commandant du Bureau central d'investigation ou le commandant régional de la police au procureur (...) compétent. Le procureur se prononce sur [la question de savoir dans quelle mesure] les données en question seront utilisées ainsi que sur leur mode d'utilisation.

6a. Le commandant en chef de la police nationale, le commandant du Bureau central d'investigation, le commandant du bureau des affaires internes de la police nationale et le commandant régional de la police peuvent autoriser leurs adjoints respectifs à procéder à la transmission prévue au paragraphe 6.

7. Les données visées au paragraphe 1 qui sont inutiles à une procédure pénale sont détruites sans délai par une commission protocolaire.

8. Les données visées au paragraphe 1 sont également mises à disposition des services répressifs des États membres de l'Union européenne et des autres pays, des agences de l'Union européenne chargées de la prévention et de la lutte contre la criminalité, de l'Organisation internationale de police criminelle - Interpol, à la demande de ces entités, lorsque cela est nécessaire à la recherche et aux poursuites d'auteurs d'infractions, au sauvetage de vies humaines ou à la protection de la santé ou à des opérations de recherche de disparus. »

Article 20cb

« 1. Dans le but de prévenir ou de détecter des infractions ou des infractions fiscales, de sauver des vies ou de protéger la santé humaine ou de mener des opérations de recherche ou de sauvetage, la police peut recueillir les données :

1,2) qui sont indiquées aux articles 161 et 179 al. 9 de la loi du 16 juillet 2004 sur les télécommunications,

3) dans les cas où l'utilisateur n'est pas une personne physique, le numéro du terminal du réseau ainsi que le siège ou l'établissement, la dénomination et la forme organisationnelle de l'utilisateur en question,

4) dans le cas où il s'agit d'un réseau public fixe de télécommunications - également le nom de la ville et de la rue où se trouve le terminal du réseau mis à la disposition de l'utilisateur,

- et peut les traiter à l'insu et sans le consentement de la personne visée.

2. Les dispositions de l'article 20c paragraphes 2-8 s'appliquent à la collecte et au traitement des données précisées à l'alinéa 1 [du présent article]. »

Article 20da

« 1. À l'occasion des opérations de recherche de disparus, la police peut conserver les données liées aux télécommunications, aux communications postales et aux communications numériques et les traiter à l'insu et sans le consentement de la personne concernée ; les dispositions de l'article 20c paragraphes 2-8 s'appliquent.

2. Les éléments qui ont été collectés dans le cadre des opérations précisées à l'alinéa 1 et sont inutiles auxdites opérations de recherche de disparus sont détruits sans délai par une commission protocolaire. »

Article 20ca

« 1. Le contrôle de l'application des mesures de conservation des données liées aux télécommunications, aux communications postales et aux communications numériques est exercé par le tribunal régional compétent au regard du siège de l'autorité de police nationale à laquelle les données en question ont été transmises.

2. L'autorité de police indiquée à l'alinéa 1 soumet au tribunal régional compétent, sous réserve des dispositions relatives à la protection des informations classifiées, un rapport semestriel indiquant :

1) le nombre de cas d'obtention de données liées aux télécommunications, aux communications postales et aux communications numériques au cours de la période considérée ainsi que le type de données recueillies ;

2) les qualifications juridiques des actes en rapport avec lesquelles les données en question ont été recueillies, ou les informations concernant les données conservées pour sauver des vies humaines ou protéger la santé ou pour soutenir des opérations de recherche ou de sauvetage.

3. Le tribunal exerçant ce contrôle peut prendre connaissance des circonstances qui ont justifié le recours par la police nationale à la conservation des données [de communication].

4. Le tribunal informe l'autorité de police des résultats de son contrôle dans un délai de trente jours à compter de l'accomplissement du contrôle en question.

5. Le contrôle susvisé ne concerne pas les données recueillies en vertu de l'article 20cb alinéa 1. »

II. LA LOI DU 24 MAI 2002 SUR L'AGENCE NATIONALE DE LA SÉCURITÉ (L'ABW) ET LES SERVICES DE RENSEIGNEMENT

Article 27

« 1. Le tribunal, statuant sur une demande écrite du chef de l'ABW préalablement approuvée par écrit par le procureur en chef du parquet national, peut ordonner un contrôle opérationnel si d'autres mesures se sont avérées inefficaces ou sont [considérées comme] inutiles - à l'occasion de la mise en œuvre par des agents de l'ABW de mesures opérationnelles d'enquête aux fins de la prévention et de la recherche des infractions indiquées :

1) à l'article 5 alinéa 1 point 2 lettres a, c, d et e,

2) aux chapitres XXXV-XXXVII du code pénal (infractions contre les biens, contre l'économie, contre le commerce de devises et de titres) et les chapitres 6-7 du code pénal fiscal –– si elles portent atteinte aux fondements économiques de l'État,

3) aux l'articles 232, 233 §§ 1, 1a, 4 et 6, 234, 235, 236 § 1 et 239 § 1 du code pénal (...) ;

- de la découverte des auteurs de ces infractions, de la recherche des preuves de leur commission et de la découverte de biens susceptibles d'une mesure de confiscation en conséquence de la commission desdites infractions.

(...)

15. En cas de recueil d'éléments de preuve rendant possible l'ouverture d'une procédure pénale ou s'avérant pertinents à l'égard de poursuites pénales en cours, le chef de l'ABW transmet au procureur en chef du parquet national général l'ensemble des éléments recueillis au moyen du contrôle opérationnel. Les dispositions de l'article 393 § 1 alinéa 1 du code de procédure pénale s'appliquent *mutatis mutandis* à la procédure devant le tribunal concernant ces éléments.

(...)

15f. Le tribunal régional de Varsovie, statuant sur une demande écrite du chef de l'ABW et sur autorisation écrite du procureur en chef du parquet national, décide de la conservation des éléments recueillis au moyen du contrôle opérationnel si ces éléments sont pertinents à l'égard de la sécurité nationale (...)

16. Les éléments qui ont été recueillis au moyen du contrôle opérationnel et qui ne sont pas pertinents à l'égard de la sécurité nationale ou ne contiennent pas de preuves de la commission d'une infraction sont détruits sans délai par une commission protocolaire. La destruction de ces éléments est ordonnée par le chef de l'ABW.

16a. Le chef de l'ABW informe sans délai le procureur en chef du parquet de la destruction des éléments visés à l'alinéa 16.

(...) »

Article 28

« 1. Les agents de l'ABW peuvent conserver les données [de communication] (...) aux fins de la réalisation des missions qui leur sont dévolues en application de l'article 5 [de la loi sur l'ABW] et ils peuvent traiter ces données à l'insu et sans le consentement de la personne visée.

(...)

6. Le chef de l'ABW transmet au procureur en chef du parquet national les données visées à l'alinéa 1 qui sont pertinentes à l'égard d'une procédure pénale. Le procureur en question décide [dans quelle mesure] ces données doivent être utilisées.

7. Les données sans pertinence à l'égard d'une procédure pénale ou de la sécurité de l'État sont détruites sans délai par une commission protocolaire. »

Article 28b

« 1. Le contrôle de l'application d'une mesure de conservation de données [de communication] (...) est exercé par le tribunal régional de Varsovie.

(...) »

III. LA LOI DU 9 JUIN 2006 SUR LE BUREAU CENTRAL DE LUTTE CONTRE LA CORRUPTION (LE CBA)

Article 17

« 1. À l'occasion de l'application par des agents du CBA de mesures opérationnelles d'enquête aux fins de la prévention ou de la découverte des infractions [mentionnées ci-après], de la découverte de leurs auteurs, de la collecte et de l'enregistrement d'éléments de preuve ou de la découverte de biens susceptibles d'une mesure de confiscation en conséquence de la commission des infractions :

1) qui sont réprimées par les articles 228-231, 250a, 258, 270a §§ 1-2, 271a §§ 1-2, 277a § 1, 286, 296-297, 299, 305 et 310 §§ 1, 2 et 4 du code pénal,

2) à la loi fiscale visées à l'article 2 alinéa 1 point 1 lettre d, si la valeur de l'objet de l'infraction ou celle de la réduction frauduleuse de la dette publique est [au moins] cinquante fois supérieure à la valeur du salaire minimum ;

3) qui sont réprimées par les articles 232, 233 §§ 1, 1a, 4 et 6, 234-235, 236 § 1 et 239 § 1 du code pénal lorsqu'elles concernent les infractions visées aux points 1 et 2 –

- dès lors que d'autres moyens paraissent inefficaces ou inutiles, le tribunal statuant sur une demande écrite formée par le chef du CBA et préalablement approuvée par le procureur en chef du parquet national peut ordonner un contrôle opérationnel.

(...)

16. Les éléments collectés au moyen du contrôle opérationnel qui ne contiennent aucune information relative à la commission d'une infraction sont détruits sans délai par une commission protocolaire. Le chef du CBA ordonne la destruction desdits éléments.

(...) »

Article 18

« 1. Les agents du CBA peuvent conserver les données [de communication] (...) et peuvent les traiter à l'insu et sans le consentement de la personne visée aux fins de l'accomplissement des missions qui leur sont dévolues en vertu de l'article 2 [de la présente loi]. »

IV. LA LOI DU 9 JUIN 2006 SUR LES SERVICES DE CONTRE-ESPIONNAGE MILITAIRE (LE SKW) ET LES SERVICES DE RENSEIGNEMENT MILITAIRE (LE SWW)

Article 31

« 1. À l'occasion de l'application par des fonctionnaires du SKW de mesures opérationnelles d'enquête aux fins d'accomplissement des missions qui leur sont dévolues en vertu de l'article 5 alinéa 1 points 1, 5, 7 et 8 et 2, dès lors que d'autres moyens paraissent inefficaces ou inutiles, le tribunal statuant sur une demande écrite formée par le chef du SKW et préalablement approuvée par le procureur en chef du parquet national peut ordonner un contrôle opérationnel.

(...)

2. La décision visée à l'alinéa 1 est rendue par le tribunal régional militaire de Varsovie (Wojskowy Sąd Okręgowy w Warszawie). »

Article 32

« 1. Le SKW peut conserver les données [de communication] aux fins d'accomplissement des missions qui lui sont dévolues en vertu de l'article 5 (...) et il peut les traiter à l'insu et sans le consentement de la personne visée.

(...)

9. Les données visées à l'alinéa 1 qui ne sont pas pertinentes à l'égard d'une procédure pénale ou de la défense de l'État font l'objet d'une destruction immédiate par une commission protocolaire. »

Article 32a

« 1. Le contrôle de l'application par les agents du SKW d'une mesure de conservation de données [de communication] est exercé par le tribunal régional militaire de Varsovie.

(...) »

V. LA LOI DU 16 NOVEMBRE 2016 SUR LE SERVICE DE CONTRÔLE FISCAL (LE KAS)

Article 115

« 1. Les fonctionnaires du KAS procédant aux mesures de contrôle opérationnel peuvent conserver des données [de communication] aux fins de la découverte des infractions à la loi fiscale qui sont précisées à l'article 2 alinéa 1 points 14 à 16 et de l'accomplissement des missions qui leur sont dévolues en vertu de l'article 2 alinéa 1 point 16a l'article 5 (...), et ils peuvent les traiter à l'insu et sans le consentement de la personne visée.

(...) »

Article 116

« 1. L'application d'une mesure de conservation de données [de communication] par des fonctionnaires du KAS est contrôlée par le tribunal régional du siège de l'autorité du KAS à laquelle les données en question ont été communiquées.

(...) »

Article 118

« 1. À l'occasion de l'application par des fonctionnaires du KAS de mesures opérationnelles d'enquête aux fins de la prévention ou de la découverte [des infractions indiquées ci-après], de la découverte de leurs auteurs ou de la collecte et de l'enregistrement d'éléments de preuve, dès lors que d'autres moyens paraissent inefficaces ou inutiles, le tribunal, statuant sur une demande écrite formée par le chef du KAS et préalablement approuvée par le procureur en chef du parquet national, peut ordonner un contrôle opérationnel [relativement aux infractions] :

1) à la loi fiscale, si la valeur de l'objet de l'infraction ou la réduction de la dette publique sont [au moins] cinquante fois supérieures au salaire minimum [en vigueur] à la date de la commission de l'infraction ;

2) fiscales qui sont réprimées par l'article 107 § 1 du code pénal fiscal ;

3) contre les échanges commerciaux, si le montant des dommages occasionnés [à la victime de ces infractions] est [au moins] cinquante fois supérieur à celui du salaire minimum [en vigueur] à la date de la commission de l'infraction ;

3a) qui sont réprimées par les articles 270a §§ 1 et 2, 271a §§ 1 et 2 et 277a § 1 du code pénal ;

4) contre les biens dont la valeur est [au moins] cinquante fois supérieure au montant du salaire minimum [en vigueur] à la date de la commission de l'infraction ;

5) qui sont réprimées par les articles 258, 270, 271 et 273 du code pénal, si la réduction frauduleuse de la dette publique en résultant représente une valeur [au moins] cinquante fois supérieure au montant du salaire minimum,

6) qui sont réprimées par les articles 228 à 231 du code pénal et ont été commises par les employés du KAS ou les agents (de celui-ci) à l'occasion de l'exercice de leurs fonctions ;

7) qui sont réprimées par les dispositions de l'article 229 du code pénal dès lors qu'elles ont été commises par les personnes autres que les employées ou les fonctionnaires du KAS (...) ;

8) qui sont réprimées en vertu tant de la législation répressive polonaise que des traités et accords internationaux ;

9) qui sont réprimées par les articles 1 à 8 et 33 § 2 du code pénal fiscal (...) ;

(...) »

Article 122

« 1. Les données précisées aux articles 114 alinéa 1 et 115 alinéa 1 et les éléments recueillis en vertu des articles 113 alinéa 1, 117 alinéa 1, 118 alinéas 1 et 3, 119 alinéas 1 et 2, 120 alinéa 1 et 127a alinéas 1 et 2 qui :

1) sont pertinents à l'égard de contrôles douaniers et fiscaux, de procédures fiscales, de procédures en matière douanière ou de procédures relatives aux infractions fiscales et aux

infractions visées à l'article 2 alinéa 1 points 14 à 16, ou aux fins de la découverte de biens susceptibles de confiscation en conséquence de la commission des infractions précisées à l'article 2 alinéa 1, points 13 à 16 ou à l'article 33 § 2 du code pénal fiscal, sont transmis à l'autorité du KAS territorialement compétente ;

2) permettent l'engagement de poursuites ou sont pertinentes à l'égard de poursuites diligentées relativement aux infractions autres que celles visées au point 1, sont transmis par le responsable du KAS ou le chef du bureau douanier et fiscal respectivement au procureur en chef du parquet national ou au procureur régional territorialement compétent (...)

(...) »

Article 123

« 1. Les données [sus]visées (...) qui n'ont pas donné lieu à des poursuites pénales ou fiscales, ou sont sans pertinence à l'égard de contrôles douaniers ou fiscaux, de procédures en matière douanière (...) ou sont inutiles aux fins de la recherche et de la découverte de biens susceptibles de confiscation en conséquence de la commission des infractions précisées à l'article 2 alinéa 1 points 13 à 16 ou à l'article 33 § 2 du code pénal fiscal, de même que les informations recueillies dans le cadre d'un contrôle opérationnel qui sont indiquées à l'article 122 alinéa 4 et dont la destruction a été ordonnée par un tribunal, sont détruites sans délai par une commission protocolaire.

2. La destruction des éléments susmentionnés, à l'exception de ceux dont la destruction a été ordonnée par un tribunal, est ordonnée par :

1) le responsable du KAS ou le chef du bureau douanier et fiscal (...),

2) le responsable du KAS (...)

3. Le responsable du KAS ou le chef d'un bureau douanier et fiscal compétent informe immédiatement le procureur en chef du parquet national ou le procureur régional compétent (...) de la destruction des données [susvisées](...) »

VI. LA LOI DU 12 OCTOBRE 1990 SUR LA POLICE DES FRONTIÈRES (LA SG)

Article 9e

« 1. À l'occasion de l'application par la police des frontières de mesures opérationnelles d'enquête aux fins de la prévention ou de la découverte [des infractions précisées ci-après], de la découverte de leurs auteurs ou de la collecte et de l'enregistrement des éléments de preuve relativement aux infractions (...) :

1) qui sont réprimées par les articles 163 § 1, 164 § 1, 165 § 1, 166 §§ 1 et 2, 167, 168, 171, 172, 173 § 1, 258, 264 §§ 2 et 3, 270a §§ 1 et 2, 271a §§ 1 et 2, l'article 277a § 1 ou 299 § 1 du code pénal,

2) qui sont réprimées par les articles 270 à 276 du code pénal et concernent des faux en documents [administratifs] permettant de franchir la frontière de l'État, en documents relatifs au droit au séjour sur le territoire de la République de Pologne ou en documents nécessaires à l'obtention de ces derniers ;

3) qui sont réprimées par l'article 134 § 1 point 1 du code pénal fiscal, lorsque la valeur de l'objet de l'infraction ou des fonds publics détournés est [au moins] cinquante fois supérieure au montant du salaire minimum (...),

4) qui sont réprimées par les articles 183 §§ 2, 4 et 5, 184 §§ 1 et 2, 263 §§ 1 et 2, 278 § 1, 291 § 1 ou 306 du code pénal, les articles 55-56 de la loi du 29 juillet 2005 sur la lutte contre la toxicomanie, les articles 44 et 46a de la loi du 1er juillet 2005 relative à la collecte, au stockage et à la transplantation de cellules, tissus et organes, l'article 109 alinéa 1 de la loi du 23 juillet 2003 sur la protection des monuments, les articles 11-13 de la loi du 13 avril 2016 relative à la sécurité du commerce des explosifs, l'article 53 alinéa 1 de la loi du 14 juillet 1983 relative à les ressources archivistiques nationales et aux archives, l'article 34a alinéa 1 de la loi du 21 novembre 1996 sur les musées ou l'article 29a alinéa 1 de la loi du 27 juin 1997 sur les bibliothèques, si l'objet de ces infractions a été exporté à l'étranger ;

5) qui sont réprimées par l'article 464 de la loi du 12 décembre 2013 sur les étrangers,

6) qui sont réprimées par les articles 228, 229 et 231 du code pénal et sont imputables aux fonctionnaires et aux employés de la police des frontières agissant dans le cadre de l'exercice de leurs fonctions, à ceux de la police nationale, à ceux des services de sécurité de l'État ou aux pompiers dans le cas indiqué à l'article 1 alinéa 2 point 4a,

6a) qui sont réprimées par l'article 229 du code pénal et ont été commises par des particuliers qui ne sont ni fonctionnaires, ni employés de la police des frontières ou de la police nationale (...),

6b) qui sont réprimées par l'article 264a du code pénal ou l'article 10 de la loi du 15 juin 2012 sur l'emploi des ressortissants étrangers en situation irrégulière,

6c) qui sont réprimées par l'article 189a du code pénal ou l'article 8 de la loi introductive du même code du 6 juin 1997,

7) qui sont réprimées en vertu tant des dispositions de la législation répressive polonaise que celles des traités et accords internationaux ;

8) qui sont réprimées par les articles 232, 233 §§ 1, 1a, 4 et 6, 234, 235, 236 § 1 et 239 § 1 du code pénal et concernent les infractions visées aux points 1 à 7 ;

9) qui sont visées aux points 1 à 8 ou réprimées par l'article 45 § 2 du code pénal ou l'article 33 § 2 du code pénal fiscal – pour autant que cela soit nécessaire à la découverte consécutive à leur commission de biens susceptibles de confiscation ;

- dès lors que d'autres moyens paraissent inefficaces ou inutiles, le tribunal, statuant sur une demande écrite préalablement approuvée par le procureur en chef du parquet national et formée soit par le chef de la police des frontières, soit par le chef du bureau des affaires internes de la police des frontières, ou sur une demande écrite du chef de la division régionale de la police des frontières préalablement approuvée par le procureur régional, peut ordonner un contrôle opérationnel.

(...) »

Article 10b

« 1. [Les fonctionnaires de] la police des frontières peuvent conserver des données [de communication] aux fins de la prévention ou de la découverte d'infractions pénales ou

d'infractions à la loi fiscale (...) et ils peuvent les traiter à l'insu et sans le consentement de la personne visée.

(...) »

Article 10ba

« 1. Le contrôle de l'application d'une mesure de conservation de données [de communication) par des fonctionnaires de la police des frontières est exercé par le tribunal régional du siège de l'autorité demanderesse.

(...) »

Articles 10bb
(la collecte des données complémentaires)

« 1. Aux fins de la prévention ou de la découverte d'infractions pénales et d'infractions à la loi fiscale, la police des frontières peut conserver les données :

1) qui sont indiquées à l'article 179 alinéa 9 de la loi du 16 juillet 2004 sur la télécommunication,

2) qui sont indiquées à l'article 161 de la loi du 16 juillet 2004 sur la télécommunication,

3) qui, dans le cas d'un utilisateur qui n'est pas une personne physique, [se rapportent] au numéro du terminal du réseau et au siège ou à l'établissement, à la dénomination et à la forme organisationnelle de cet utilisateur,

4) qui, dans le cas d'un réseau public fixe de télécommunications - concernent le nom de la ville et de la rue où se trouve le terminal du réseau mis à la disposition de l'utilisateur,

- et elle peut les traiter à l'insu et sans le consentement de la personne visée.

2. Les dispositions de l'article 10b alinéas 2-8 s'appliquent à la conservation et au traitement des données mentionnées à l'alinéa 1. »

VII. LA LOI DU 24 AOÛT 2001 SUR LA POLICE MILITAIRE (LA ŻW) ET LES CELLULES DE RÉPRESSION MILITAIRE

Article 30

« 1. [Les fonctionnaires de] la police militaire peuvent conserver des données [de communication] aux fins de la prévention ou de la découverte des infractions pénales et des infractions à loi fiscale qui ont été commises par les personnes indiquées à l'article 3 alinéa 2 points 1, 3, 4, 5 et 6, du sauvetage de vies humaines ou de la protection de la santé, ou encore de la réalisation d'opérations de recherche et de sauvetage, (...) et ils peuvent les traiter à l'insu et sans le consentement de la personne visée.

(...) »

Article 30b

« 1. Le contrôle de l'application par des fonctionnaires de la police militaire d'une mesure de conservation de données [de communication] est exercé par le tribunal régional du siège de l'autorité de la police militaire à laquelle ces données ont été communiquées.

(...) »

Article 31

« 1. À l'occasion de l'application par des fonctionnaires de la police militaire de mesures opérationnelles d'enquête aux fins de l'accomplissement des missions qui leur sont dévolues en application de l'article 4 alinéa 1 relativement aux individus indiqués à l'article 3 alinéa 2 points 1, 3, 5 et 6, et de la prévention ou de la découverte [des infractions précisées ci-après], de la découverte de leurs auteurs ou de la collecte ou de l'enregistrement des éléments de preuves [relativement aux infractions]:

1) contre la paix et l'humanité,

2) contre la République de Pologne, à l'exception de celles qui sont réprimées par l'article 127-132 du code pénal,

3) contre la vie qui sont réprimées par les articles 148-150 du code pénal,

4) réprimées par les articles 140, 156 §§ 1 et 3, 163 §§ 1 et 3, 164 § 1, 165 §§ 1 et 3, 166, 167, 171 § 1, 173 §§ 1 et 3, 189, 189 *bis*, 200, 200a, 202 §§ 3 et 4, 211a, 223, 228 §§ 1 et 3-5, 229 §§ 1 et 3-5, 230 § 1, 230a § 1, 231 §§ 1et 2, 232, 233 §§ 1, 1 *bis*, 4 et 6, 234, 235, 236 § 1, 238, 239 § 1, 240 § 1, 245, 246, 252 §§ 1-3, 258, 263 §§ 1 et 2, 265, 269, 270a §§ 1 et 2, 271a §§ 1 et 2, 277a § 1, 280-282, 285 § 1, 286 §§ 1 et 2, 299 §§ 16, 305, 310 §§ 1, 2 et 4, 339 § 2, 345 §§ 2 et 3 et 358 § 2 du code pénal,

5) à la loi fiscale, si la valeur de l'objet de l'infraction ou des fonds publics détournés est [au moins] cinquante fois supérieure au montant du salaire minimum (...) ;

6) qui sont réprimées par l'article 8 de la loi introductive au code pénal du 6 juin 1997 ;

6a) listées aux chapitres 11 de la loi du 23 juillet 2003 sur la protection des monuments, 5 de la loi du 14 juillet 1983 sur les ressources archivistiques nationales et les archives, 6 de la loi du 25 mai 2017 sur la restitution des biens culturels nationaux, 5a de la loi du 21 novembre 1996 sur les musées et 11a de la loi du 27 juin 1997 sur les bibliothèques ;

7) listées aux articles 43 et 44 de la loi du 1er juillet 2005 sur le recueil, la conservation et la transplantation de cellules, tissus et organes,

8) qui sont réprimées par les articles 53 alinéa 1, 55 alinéa 1, 56 alinéa 1, 58 alinéa 1, 59 alinéa 1, 62 alinéa 1 et 62b alinéas 1 et 2 de la loi du 29 juillet sur la lutte contre la toxicomanie,

9) qui sont réprimées tant par les dispositions de la législation répressive nationale que par des traités et accords internationaux,

- dès lors que d'autres moyens paraissent inefficaces ou inutiles, le tribunal régional militaire, statuant sur une demande écrite formée par le chef de police militaire préalablement approuvée par le procureur en chef du parquet national, ou sur celle du chef de la division régionale de la police militaire préalablement approuvée par le procureur régional compètent en matière militaire, peut ordonner un contrôle opérationnel.

(...)

21. Le contrôle opérationnel dont la mise en application a été autorisée en vertu de la présente loi est diligenté (...) par les fonctionnaires du SKW.

(...) »

---

[1] La loi du 6 avril 1990 sur la police, la loi du 24 mai 2002 sur l'ABW et les services de renseignement, la loi du 9 juin 2006 sur le CBA, la loi du 9 juin 2006 sur le SKW et le service de renseignement militaire, la loi du 16 novembre 2016 sur le KAS, la loi du 12 octobre 1990 sur la SG, la loi du 24 août 2001 sur la ŻW et les cellules de répression militaire (*Ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych*).

[2] Selon les articles 15f et 16 de la loi sur l'ABW et les services de renseignement, les services de l'ABW peuvent conserver les éléments recueillis au moyen du contrôle opérationnel qui sont pertinents à l'égard de la sécurité nationale. Par ailleurs, l'article 123 de la loi sur le KAS indique que les services de le KAS peuvent conserver les informations obtenues au moyen d'un contrôle opérationnel qui sont pertinentes à l'égard d'une procédure diligentée relativement aux infractions à la loi fiscale.

[3] Les services de l'ABW et ceux de renseignement militaire peuvent en outre conserver les données de communication qui sont pertinentes respectivement à l'égard de la sécurité et la défense nationales (l'article 28 de la loi sur l'ABW et les services de renseignement et l'article 32 de la loi sur le SKW et le service de renseignement militaire).

[4] Une prolongation peut être ordonnée par une décision de justice, à la demande du chef de l'ABW et sur autorisation écrite du procureur en chef du parquet national, pour une période supplémentaire de trois mois. Dans les cas dument justifiés, la surveillance peut être prolongée par une juridiction compétente pour plusieurs périodes consécutives pour une durée maximale globale de douze mois.

[5] La loi sur la police, celle sur l'ABW, celle sur le CBA, celle sur le SKW et le service de renseignement militaire, celle sur la SG et celle sur la ŻW

[6] Programme permettant une collecte quasi systématique des activités de tout utilisateur sur Internet.

[7] Les États suivants sont concernés : Albanie, Arménie, Azerbaïdjan, Belgique, Bosnie-Herzégovine, Croatie, République Tchèque, Estonie, France, Géorgie, Grèce, Allemagne, Hongrie, Islande, Irlande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, République de Moldova, Monténégro, Pays-Bas, Macédoine du Nord, Norvège, Portugal, Roumanie, San Marin, Serbie, République Slovaque, Slovénie, Espagne, Suède, Suisse et Royaume-Uni

[8] Albanie, Arménie, Azerbaïdjan, Belgique, Bosnie-Herzégovine, République Tchèque, Estonie, France, Géorgie, Grèce, Allemagne, Hongrie, Islande, Irlande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, République de Moldova, Monténégro, Pays-Bas, Macédoine du Nord, Norvège, Roumanie, San Marin, Serbie, Slovénie, Espagne et Suède

[9] Belgique, Hongrie, Luxembourg, République de Moldova, Monténégro, Serbie, Slovénie et Espagne

[10] Estonie

[11] République Tchèque et Macédoine du Nord

[12] Norvège, Suède et Macédoine du Nord

[13] Albanie, Arménie, Azerbaïdjan, Croatie, République Tchèque, Estonie, Hongrie, Irlande, Lettonie, Lituanie, Luxembourg, Macédoine du Nord, Norvège, Roumanie, Serbie, République Slovaque, Slovénie et Suisse

[14] Grèce, Italie et Liechtenstein.

[15] Belgique, France, Allemagne, Luxembourg, Pays-Bas et Royaume-Uni

[16] France, Irlande, Serbie, Slovénie et Royaume-Uni

[17] Croatie, République Tchèque, Estonie, Allemagne, Italie, Lettonie, Lituanie, Luxembourg, Macédoine du Nord, Norvège, Roumanie, Slovaquie et Slovénie

[18] Belgique, Croatie, République Tchèque, France, Allemagne, Grèce, Pays-Bas et Macédoine du Nord

[19] Croatie, Lettonie et Luxembourg

[20] Estonie, Allemagne, Hongrie, Liechtenstein, Pays-Bas, Roumanie, Slovénie et Suisse

[21] Albanie, Estonie, Géorgie, Hongrie, Italie, Lettonie, Luxembourg, Slovénie et Suisse

[22] Belgique, France, Grèce, Irlande, Pays-Bas, Suède et Royaume-Uni.

[23] Bosnie-Herzégovine, Croatie, Estonie et Lituanie

[24] Albanie, Arménie, Belgique, République Tchèque, Estonie, France, Hongrie, Irlande, Liechtenstein, Lituanie, Luxembourg, République de Moldova, Macédoine du Nord, Norvège, Serbie, République Slovaque, Espagne, Suède, Suisse et Royaume-Uni

[25] Albanie, République Tchèque, Estonie, France, Hongrie, Irlande, Lituanie, Luxembourg, République de Moldova, Norvège, Serbie, République Slovaque, Espagne, Suède, Suisse et Royaume-Uni

[26] Arménie, Belgique et Macédoine du Nord

[27] Belgique, Bosnie-Herzégovine, Estonie, France, Géorgie, Allemagne, Hongrie, Irlande, Lettonie, Liechtenstein, République de Moldova, Pays-Bas, Macédoine du Nord, Norvège, République Slovaque, Slovénie, Suède, Suisse et Royaume-Uni

[28] À la différence de la surveillance ciblée, la surveillance stratégique n'est pas forcément déclenchée en raison d'un soupçon pesant sur une ou plusieurs personnes spécifiques. Elle vise à trouver ou à identifier un danger au lieu d'enquêter uniquement sur une menace connue.

[29] Bosnie-Herzégovine, Estonie, Géorgie, Hongrie, Irlande, Lettonie, République de Moldova, Macédoine du Nord, Norvège, République Slovaque et Suisse

[30] Belgique et Slovénie

[31] Bosnie-Herzégovine, Estonie, Lettonie, Macédoine du Nord, Norvège, République Slovaque et Slovénie

[32] France, Irlande, République de Moldova et Royaume-Uni

[33] Belgique, France, Liechtenstein, Pays-Bas, Macédoine du Nord et Suède

[34] Bosnie-Herzégovine et Lettonie

[35] Bosnie-Herzégovine, Estonie, Géorgie, Hongrie et Irlande

[36] Belgique, France, Grèce, Irlande, Pays-Bas, Suède et Royaume-Uni

[37] Bosnie-Herzégovine, Croatie, Estonie et Lituanie

[38] Des ONG ayant une grande expertise dans les aspects techniques de la surveillance ont informé de nombreuses personnes à travers le monde, y compris des citoyens polonais, qu'elles étaient victimes d'un logiciel espion hautement intrusif (une arme cybernétique).

[39] A/HRC/10/3

[40] A/HRC/14/46

[41] "Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'UE" du 6 novembre 2015 ; « Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'UE – volume II : situation sur le terrain et évolution juridique », du 20 octobre 2017.

[42] Le présent document reprend les dispositions pertinentes de la loi sur la police et des lois portant réglementation des autres services de l'État ayant recours à la surveillance secrète (pour autant qu'elles soient différentes des dispositions pertinentes de la loi sur la police) dans leur formulation applicable à l'époque des faits.