Strasbourg, 13 juin 2016 **CDL-AD(2016)012**

Avis n° 839/2016 Or. anglais

COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT

(COMMISSION DE VENISE)

POLOGNE

AVIS

RELATIF A LA LOI DU 15 JANVIER 2016 PORTANT MODIFICATION DE LA LOI SUR LA POLICE ET DE CERTAINES AUTRES LOIS

adopté par la Commission de Venise
à sa 107e session plénière
(Venise, 10-11 juin 2016)

sur la base des observations de

M. Iain CAMERON (membre, Suède)
Mme Regina KIENER (membre, Suisse)
M. Ben VERMEULEN (membre, Pays-Bas)

TABLE DES MATIÈRES

I. Introduction

1. Le Président de la Commission de suivi de l'Assemblée parlementaire[1] a demandé dans sa lettre du 29 janvier 2016 à la Commission de Venise un avis sur la loi polonaise du 15 janvier 2016 portant modification de la loi sur la police et de certaines autres lois. Ces modifications sont entrées en vigueur le 7 février 2016, comme le prévoyait leur article 17.

2. M. Iain Cameron, Mme Regina Kiener et M. Ben Vermeulen ont été invités à être rapporteurs pour cet avis. Une délégation de la Commission de Venise s'est rendue les 28 et 29 avril 2016 à Varsovie, où elle a eu des entretiens avec des autorités publiques, des membres de la classe politique, des juristes et des représentants d'ONG. La Commission de Venise remercie le ministère des Affaires étrangères de l'excellente organisation de cette visite.

3. Le présent avis s'appuie sur les observations des rapporteurs, elles-mêmes fondées sur une traduction en langue anglaise de la loi sur la police et d'autres textes législatifs (CDL-REF(2016)036). Ces traductions pouvant ne pas refléter en tout point le sens de la version originale du texte, certaines observations pourraient trouver leur origine dans des problèmes de traduction.

4. Le présent avis a été adopté par la Commission de Venise à sa 107e session plénière (Venise, 10 et 11 juin 2016).

II. Portée de l'analyse

5. Les amendements de 2016 visaient à codifier des méthodes de surveillance secrète[2] employées par les services de police et de renseignement. Des organismes de l'Etat 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[3], c'était le pouvoir donné aux organismes de l'Etat 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[4].

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

[1] Commission pour le respect des obligations et engagements des Etats membres (de l'Assemblée parlementaire du Conseil de l'Europe).

[2] Le terme de surveillance est utilisé ici dans deux sens : au sens général pour désigner toutes les formes de collecte secrète d'informations, et dans un sens plus étroit de surveillance cachée du *contenu* de communications privées (par opposition à la collecte de métadonnées : pour la distinction, se reporter aux paragraphes 14 et suivants).

[3] En Pologne, les modifications apportées à la loi sur la police et à d'autres textes ont été très critiquées, notamment par le Médiateur polonais, l'Inspecteur général pour la protection des données, le Conseil national de la justice, le Conseil du barreau et des députés d'opposition. Certaines organisations de la société civile dignes de foi ont affirmé que la nouvelle législation, sous couvert de mettre en œuvre l'arrêt de juillet 2014 de la Cour constitutionnelle, renforçait les pouvoirs de surveillance dans de nombreux domaines et était incompatible avec des obligations internationales de la Pologne en matière de droits de l'homme. Le 13 janvier 2016, l'Union européenne a annoncé son intention d'entamer un dialogue structuré avec les autorités polonaises dans le contexte de son Cadre pour l'Etat de droit, afin de déterminer s'il convenait d'invoquer l'article 7 du Traité de l'UE pour sauvegarder les valeurs et normes européennes dans le sillage de l'adoption récente de plusieurs lois en Pologne, dont les modifications apportées à la loi sur la police. La Commission de Venise constate que la Pologne n'est pas seule à s'attirer des critiques pour sa législation sur la surveillance ; voir par exemple Comité des droits de l'homme des Nations unies, *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland of 2015*, point 24 ; *Concluding observations on the fifth periodic report of France*, 2015, point 12 ; *Concluding observations on the fourth periodic report of the United States of America*, 2014, point 22.

[4] L'avis abordera également l'interception secrète de conversations en direct ; se reporter à l'analyse de l'article 19 de la loi sur la police (paragraphes 13 et 14 du présent avis).

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[5]. Mais le renseignement est un domaine extrêmement complexe et délicat, qui mérite une analyse à part[6].

7. Les modifications de 2016 concernaient plusieurs lois portant sur les activités de services de police et de renseignement[7]. Tous ces textes prévoient en fin de compte le même modèle de surveillance (à quelques petites exceptions près)[8]. 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[9].

8. La Commission de Venise sait que le Tribunal constitutionnel de Pologne procède actuellement au contrôle de constitutionnalité des modifications de 2016 (affaire n° K 9/16), à la suite d'une requête déposée par le Commissaire aux droits de l'homme, M. Adam Bodnar. Par égard pour le Tribunal constitutionnel, elle ne se prononcera pas sur la compatibilité des modifications de 2016 avec la Constitution polonaise, et fondera son analyse sur les normes internationales en la matière et sur des exemples d'autres pays permettant de les illustrer.

9. Le présent avis ne constitue donc pas une évaluation exhaustive de tous les aspects des modifications. Il fait ressortir un certain nombre de problématiques qui ont attiré l'attention à l'intérieur et à l'extérieur du pays, et sur lesquelles selon l'avis de la Commission de Venise, le législateur polonais devrait se repencher en priorité.[10].

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 n° K 23/11 du 30 juillet 2014 du Tribunal constitutionnel de Pologne, où ce dernier déclarait certaines dispositions du texte original de la loi de 1990 sur la police (et de plusieurs autres lois) incompatibles avec la Constitution polonaise. Il avait procédé à une analyse soigneuse et convaincante du cadre juridique intérieur et des normes internationales relatives à la surveillance[11]. Il est inutile de reproduire ici le détail de son raisonnement ; qu'il suffise de rappeler les grands principes formulés au paragraphe 5.3 de l'arrêt, dont devait tenir compte la

---

[5] Voir CDL-AD(2015)011, Rapport sur le contrôle démocratique des agences de renseignement d'origine électromagnétique, paragraphe 33 (ci-après désigné par « le rapport de 2015 »). Pour une analyse du droit européen, voir le rapport de 2015 de l'Agence des droits fondamentaux de l'Union européenne *Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'Union européenne; Panorama du droit des Etats membres*, paragraphes 10 et 11 (document en anglais, résumé en français).

[6] La Commission de Venise n'abordera pas non plus la surveillance extraterritoriale et les échanges d'informations entre services de sécurité nationaux (dans le contexte polonais, voir l'article 20, paragraphe 2ab, de la loi). Elle sait qu'ils figurent parmi les procédés parfois utilisés pour contourner les règles nationales applicables à la surveillance, mais la question ne semble pas être au cœur du débat intérieur suscité par les récentes modifications, et ne sera donc pas analysée.

[7] 1) La loi du 6 avril 1990 sur la police ; 2) la loi du 12 octobre 1990 sur la garde des frontières ; 3) la loi du 28 septembre 191 sur les contrôles fiscaux ; 4) la loi du 21 août 1997 sur le système de tribunaux militaires ; 5) la loi du 27 juillet 2001 sur le système des juridictions de droit commun, 6) la loi du 24 août 2001 sur la police militaire et les cellules de répression militaire, 7) la loi du 24 mai 2002 sur l'agence nationale de la sécurité et l'agence nationale de renseignement ; 8) la loi du 18 juillet 2002 sur la fourniture de services par des moyens électroniques ; 9) la loi du 16 juillet 2004 sur les télécommunications ; 10) la loi du 9 juin 2006 sur le service de contre-espionnage militaire et le service de renseignement militaire ; 11) la loi du 9 juin 2006 sur le bureau central de lutte contre la corruption ; 12) la loi du 27 août 2009 sur le bureau des douanes.

[8] La loi modifie les textes relatifs à divers bureaux et services susceptibles de se livrer à des surveillances secrètes, mais aussi plusieurs autres textes qui traitent de la mise en œuvre des mesures de surveillance.

[9] La police, le corps des gardes-frontières, le service de contrôle fiscal, la police militaire, l'agence nationale de sécurité et l'agence nationale de renseignement, le service de contre-espionnage militaire et le service de renseignement militaire, le bureau central de lutte contre la corruption et le bureau des douanes.

[10] Les autorités polonaises ont communiqué le 7 juin 2016 leur position sur les questions abordées dans le présent avis.

[11] L'arrêt peut être consulté dans une traduction anglaise sur le site Web du Tribunal constitutionnel : http://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/

révision de la législation sur la surveillance secrète, et qui peuvent être synthétisés comme suit :

- la loi devrait contenir des dispositions explicites et précises sur son champ d'application matériel, et énumérer les organismes habilités à collecter des informations par surveillance secrète et à les traiter ;
- elle devrait préciser les types d'infractions justifiant le recours à des mesures de recherche d'informations comme la surveillance secrète, et ces infractions devraient être suffisamment graves pour justifier le recours à la surveillance secrète ;
- elle devrait préciser la durée maximale des mesures de surveillance et, si possible, les moyens techniques envisagés pour obtenir l'information[12] ;
- elle devrait définir la procédure d'autorisation de ces mesures par une autorité indépendante, et mettre en place un dispositif de contrôle indépendant de l'obtention et du traitement des données relatives à des personnes ;
- elle devrait contenir une obligation de destruction des documents non pertinents ou non admissibles, préciser la procédure à suivre dans ce contexte, et mettre en place des garanties contre la consultation non autorisée d'informations obtenues par surveillance secrète ;
- elle devrait garantir le droit de la personne surveillée d'être informée dans un délai raisonnable de cette surveillance une fois que cette dernière a pris fin, et le droit de demander un contrôle juridictionnel, avec dérogations possibles à l'obligation de notification dans des cas exceptionnels ;
- les services concernés devraient publier des données statistiques sur la surveillance secrète permettant une analyse de son intensité ;
- la loi pourrait contenir des règles spécifiques relatives à la surveillance secrète exercée par les services de renseignement et de sécurité de l'Etat (par opposition à la police) et à la collecte de données relatives à des ressortissants non polonais.

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 infractions (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[13]. La surveillance secrète *précède* fréquemment, pour la justifier, l'ouverture d'une enquête. Mais toute surveillance

[12] La partie afférente du paragraphe 5.3 dit qu'il est souhaitable d'indiquer ces moyens techniques ; il en découle qu'il ne s'agit pas d'une exigence stricte, mais plutôt d'une recommandation.

[13] Le chapitre 26 du Code de procédure pénale traite de la collecte d'éléments de preuve par surveillance secrète pour une procédure pénale déjà ouverte.

secrète ne débouche pas sur l'ouverture d'une procédure pénale[14]. En revanche, les informations obtenues par surveillance secrète peuvent être présentées comme éléments de preuve dans les procédures pénales[15]. 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[16].

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)[17].

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[18]. 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).

---

[14] Le Commissaire des droits de l'homme a fait valoir le 18 février 2016 dans sa requête au Tribunal constitutionnel de Pologne concernant l'inconstitutionnalité des modifications de la loi sur la police (pages 7 et 8) que les dispositions concernées (articles 19 et autres) ne concernent pas des activités opérationnelles et des investigations menées dans le cadre de la procédure pénale comme le prévoit le Code de procédure pénale ; que les dispositions faisant l'objet de sa requête portent sur des activités ne relevant pas de la procédure pénale, tout en pouvant déboucher sur des poursuites pénales, mais pas nécessairement ; que les études publiées montrent bien que la surveillance opérationnelle joue un rôle subsidiaire dans les procédures pénales, et qu'elle précède la procédure préparatoire, dont elle justifie l'ouverture.

[15] Voir, par exemple, le paragraphe 15g de l'article 19, qui décrit les conditions dans lesquelles des informations extraites de communications couvertes par le secret professionnel peuvent être utilisées dans une procédure pénale.

[16] La Commission de Venise rappelle que l'article 19 de la loi parle d'accès *secret* au contenu de la correspondance, de lettres, d'e-mails, etc. Dans certains pays, les services de répression peuvent aussi procéder à la surveillance *déclarée* des communications de certains groupes de personnes, le plus souvent les prisonniers. Le présent avis n'aborde pas les ingérences dans la vie privée que peut constituer ce type de surveillance.

[17] Voir le document CDL-REF(2016)036, qui contient des extraits de la législation concernée (en langue anglaise).

[18] La liste est trop longue pour être reproduite intégralement ; pour plus de détails, se reporter au document CDL-REF(2016)036.

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)[19]. La Commission de Venise rappelle que la Pologne possède une population de plus de 38 millions d'habitants.

21. Avant de passer à l'examen détaillé de la loi sur la police, 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)[20], 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)[21].

[19] Les autorités polonaises indiquent que les chiffres ci-dessus s'expliquent en partie par le fait qu'il n'existe pas de base de données centrale des abonnés pour la téléphonie portable : les demandes concernant une personne doivent donc être soumises à plusieurs opérateurs. De même, un grand nombre de demandes de consultation d'autres sortes de métadonnées peuvent aussi concerner une seule et même personne.

[20] Auparavant, l'alinéa 3 du paragraphe 6 de l'article 19 autorisait la mise en œuvre de mesures techniques facilitant l'obtention secrète d'informations et d'éléments de preuve, ainsi que leur enregistrement, en particulier le contenu de conversations téléphoniques et autres informations transmises sur les réseaux de télécommunications. Le Tribunal constitutionnel avait donné à cette disposition une interprétation large dans son arrêt du 30 juillet 2014 (paragraphe 6.1.2), où il estimait que les dispositions contestées, interprétées textuellement, rendaient notamment possible la surveillance audio de personnes et de locaux, avec interception de conversations sur les lignes téléphoniques terrestres, ainsi que par téléphonie portable et Internet ; l'interception de SMS et de messages multimédias transmis par matériel téléphonique ou autre de télécommunications ; le recours à du matériel capable de localiser des personnes et des objets par navigation satellite ; ou l'interception de signaux électromagnétiques.

[21] Il existe des règles spéciales applicables à la surveillance exercée par les services de contre-espionnage militaire et les services de la sécurité intérieure.

V. A quel degré les mesures prévues aux articles 19 et 20c de la loi constituent-elles une ingérence dans la vie privée ?

22. L'article 8 de la Convention européenne des droits de l'homme (CEDH) protège le droit au respect de la vie privée et à la confidentialité des communications. La Cour européenne des droits de l'homme a précisé au fil des ans la notion de « vie privée », qui englobe à présent le droit à la confidentialité de certaines informations à caractère personnel[22].

23. Il est impossible de donner une définition simple et complète de ce que serait une information à caractère privé. La vie privée est un concept social complexe, qui évolue avec le temps et varie d'un pays à l'autre[23]. Il n'en reste pas moins que le *contenu* des communications privées était originellement et reste toujours au cœur de la protection garantie par l'article 8 de la Convention. De plus, certaines mesures de surveillance secrète décrites dans la loi peuvent aussi impliquer des ingérences au domicile (le paragraphe 6, alinéa 2, de l'article 19 évoque par exemple la possibilité d'obtenir et d'enregistrer des images ou des sons de personnes dans des pièces, ce qui implique clairement la pose de microphones invisibles dans des lieux de vie). Les mesures de surveillance prévues à l'article 19 de la loi constituent donc bien une ingérence aux droits garantis à l'article 8[24].

24. En ce qui concerne la collecte de *métadonnées*, la situation est moins claire. Jusqu'à une période relativement récente, les métadonnées étaient considérées comme moins sensibles que le contenu des communications en ce qui concerne l'intégrité de la personne[25].

25. Mais l'arrivée de l'Internet, des téléphones intelligents et autres dispositifs portables a transformé la façon dont sont perçues les métadonnées. L'empreinte numérique que laisse la personne derrière elle permet souvent d'obtenir sur elle un grand nombre d'informations à caractère personnel par collecte de métadonnées et analyse combinée de ses modes de communication. Les organes de contrôle ont observé que les services de police recourent moins aux méthodes intrusives de collecte d'informations (écoutes téléphoniques, etc.) parce qu'ils peuvent obtenir les mêmes renseignements par les médias sociaux[26]. De plus, il existe un espace d'interaction d'une personne avec d'autres qui pourrait bien, même s'il est public, relever de la « vie privée »[27] ; l'information sur son cercle d'amis proches pourrait, par exemple, mériter une protection.

---

[22] Voir également l'observation générale n° 16 relative au PIDCP : Article 17 (droit au respect de la vie privée), en particulier les points 10 et 11 (adopté le 8 avril 1988 à la 32e session du Comité des droits de l'homme).

[23] Dans *Uzun c. Allemagne*, la Cour européenne des droits de l'homme avait rappelé que « la "vie privée" est une notion large, qui ne se prête pas à une définition exhaustive » (no 35623/05, paragraphe 43, CrEDH 2010, extraits).

[24] De plus, la surveillance peut aussi porter indirectement atteinte à d'autres droits de l'homme dont la réalisation dépend du droit à la vie privée, notamment la liberté d'expression (article 10 de la Convention, en particulier en ce qui concerne le droit des journalistes à ne pas révéler leurs sources ; voir *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, n° 39315/06, 22 novembre 2012). Si la surveillance débouche sur l'interception de communications confidentielles avec un avocat ou un prêtre, la loi pourrait aussi enfreindre le principe du droit à un procès équitable (article 6 de la Convention) et la liberté de religion (article 9 de la Convention).

[25] Voir le rapport de 2007, paragraphe 202, et le rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique (CDL-AD(2015)011), paragraphe 41 (ci-après désigné par « rapport de 2015 »). Voir également l'arrêt de la Cour européenne des droits de l'homme en l'affaire *PG et JH c. Royaume-Uni*, n° 44787/98, 25 septembre 2001 ; la Cour avait notamment observé qu'en l'espèce, « les renseignements obtenus avaient trait aux numéros de téléphone appelés à partir de l'appartement de B. entre deux dates particulières. Ils ne comprenaient aucune information sur le contenu de ces appels, ou sur l'identité des personnes qui les avaient passés ou reçus. Les données recueillies et l'utilisation qui pouvait en être faite étaient donc strictement limitées. » (paragraphe 46).

[26] Voir par exemple le rapport annuel du *Chief Surveillance Commissioner* du Royaume-Uni au Premier ministre et aux ministres écossais pour 2011-2012, en 5.17, dans lequel il expliquait que ses inspecteurs se voyaient fréquemment répondre, lorsqu'ils s'enquéraient de la réduction de la surveillance directe, que les investigations non secrètes sur l'Internet suffisaient ; les inspecteurs s'étaient alors inquiétés du fait que certaines recherches fondées sur l'Internet pouvaient constituer une surveillance ciblée, surtout si le traitement des données permettait de retrouver le profil d'une personne ou d'un groupe à leur insu.

[27] *Uzun c. Allemagne*, citée précédemment, paragraphe 43

26. On pourrait tenter de classer les métadonnées en fonction du degré auquel leur interception peut constituer une ingérence dans la vie privée. Les données révélant simplement l'identité du titulaire de l'abonnement téléphonique appartiendraient par exemple à une catégorie moins sensible. D'autres métadonnées se rapprochent beaucoup d'une information sur le contenu des communications privées et peuvent être qualifiées de « se rapportant au contenu » (les renseignements permettant par exemple de retrouver les sites Internet qu'a consultés une personne). Les données de localisation géographique des dispositifs mobiles peuvent être plus ou moins sensibles, selon la situation. Le lieu dans lequel se trouve une personne à un moment donné peut être connu par le simple fait que ladite personne a été vue dans un lieu public, ce qui diminuerait l'attente de confidentialité. Mais le suivi systématique de tous les mouvements d'une personne pendant une période donnée, voire en temps réel, constitue une intrusion beaucoup plus profonde dans sa vie privée[28].

27. La Commission de Venise constate toutefois que les progrès constants de la technologie dans ce domaine invitent à ne pas multiplier les distinctions entre catégories de données. Il est en tout cas clair que la *combinaison* de plusieurs types de métadonnées (se rapportant au contenu, comme la journalisation des sites Web et la localisation en continu, par exemple) permet de se faire une idée assez complète des habitudes d'une personne, de ses centres d'intérêt, de ses relations, etc., comme l'a montré l'expérience faite par un membre de la classe politique allemande qui avait installé sur son téléphone un logiciel espion pendant un mois[29].

28. En l'affaire *Digital Rights Ireland v. Minister for Communications & Others*[30], la Cour de justice de l'Union européenne a examiné la compatibilité de la directive européenne sur la conservation des données avec les articles 7 (respect de la privée et de la vie familiale) et 8 (protection des données à caractère personnel) de la Charte des droits fondamentaux de l'Union européenne. Dans son arrêt, la Cour a dit ce qui suit :

> *26. A cet égard, il convient de relever que les données que doivent conserver les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, au titre des articles 3 et 5 de la directive 2006/24, sont, notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.*
>
> *27. Ces données,* ***prises dans leur ensemble*** [c'est nous qui soulignons]*, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.*

29. Ce qui veut dire que la Cour a estimé que la divulgation de ce type d'information, compte tenu de ses effets cumulés, constitue clairement une ingérence dans la vie privée, que protège l'article 7 de la Charte. Elle a donc invalidé la directive sur la conservation des données, et

---

[28] Voir le raisonnement de la Cour européenne des droits de l'homme en l'affaire *Uzun c. Allemagne*, citée précédemment, où la Cour analysait les effets de la surveillance secrète des mouvements d'une personne à l'aide d'un récepteur GPS installé dans une voiture qu'elle utilisait régulièrement.

[29] Voir https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/

[30] Affaires C-293/12 et C-594/12, 8 avril 2014

plusieurs juridictions ont suivi son exemple au sein de l'UE, en insistant sur la nécessité de mieux contrôler la collecte de métadonnées[31].

30. La Cour européenne des droits de l'homme estime également que l'article 8 de la CEDH s'applique de façon assez large à ce type de données. L'exploitation d'informations se rapportant à la date et à la durée des conversations téléphoniques, et notamment aux numéros composés, peut contrevenir à l'article 8, ces éléments faisant « partie intégrante des communications téléphoniques »[32]. De plus, la collecte systématique et la conservation par les services de sécurité de données relatives à un individu, même sans recours à des méthodes de surveillance secrète, constituent une ingérence dans sa vie privée[33].

31. En ce qui concerne la Pologne, la Commission de Venise constate que les données collectées en application de l'article 20c de la loi[34] 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[35].

VI. Garanties procédurales et matérielles contre la surveillance abusive

A. Normes internationales

32. Les normes internationales en matière de droits de l'homme, en particulier la CEDH, imposent que toute mesure visant à obtenir une information à caractère privé poursuive des buts légitimes, soit prévue par la loi et nécessaire dans une société démocratique (article 8, paragraphe 2, de la CEDH). En ce qui concerne le but légitime, il ne fait aucun doute que les buts de la surveillance secrète prévue à l'article 19 et de la collecte de métadonnées prévue à l'article 20c de la loi sur la police sont compatibles avec la norme à cet égard[36].

---

[31] Voir, Cour constitutionnelle d'Autriche, décision dans l'affaire G 47/2012 et autres du 27 juin 2014. Dans certains cas, les décisions négatives ont précédé celle de la Cour de justice européenne ; voir en particulier l'arrêt de la Cour constitutionnelle fédérale allemande dans 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 du 2 mars 2010 sur la directive relative à la conservation des données.

[32] *Copland c. Royaume-Uni*, n° 62617/00, paragraphe 43, CrEDH 2007-I; voir également *Malone c. Royaume-Uni*, 2 août 1984, paragraphe 84, série A n° 82; voir aussi l'opinion séparée du juge Pinto de Albuquerque en l'affaire *Bărbulescu c. Roumanie,* n° 61496/08*, 12 janvier 2016*, qui concluait que la protection de l'article 8 couvre non seulement le contenu des communications, mais aussi les métadonnées obtenues par collecte et conservation des données de communication et qui peuvent permettre de connaître le mode de vie d'une personne, ses croyances religieuses, ses opinions politiques, ses préférences personnelles et ses relations sociales.

[33] Voir *Rotaru c. Roumanie* [GC], n° 28341/95, paragraphes 43-44, CrEDH 2000-V; *Amann c. Suisse* [GC], n° 27798/95, paragraphes 65-67, CrEDH 2000-II (la conservation d'informations sur la fiche d'un candidat avait été jugée constituer une ingérence dans sa vie privée, alors qu'il ne s'agissait pas de renseignements sensibles et qu'ils n'avaient probablement jamais été consultés).

[34] Pour une description exacte de ce que englobe la notion de métadonnées en droit polonais, voir le document CDL-REF(2016)036 ; voir également l'analyse présentée aux paragraphes 60 et suivants du présent avis.

[35] Voir, à titre d'exemple, *Copland*, cité précédemment, paragraphes 41-44.

[36] La mesure doit être « 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 ».

33. Toute ingérence doit par ailleurs être prévue dans la loi. Cette exigence de légalité contient implicitement le critère de clarté et de prévisibilité de la loi[37]. Dans l'arrêt de la Grande chambre en l'affaire *Roman Zakharov c. Russie*[38], la Cour européenne des droits de l'homme a ainsi résumé sa jurisprudence sur la question de la prévisibilité dans le contexte de l'interception de communications : « La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes ». Elle a ajouté que « puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la "loi" irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ou à un juge ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire. » (paragraphes 229 et 230)

34. Le dernier critère, le plus complexe, qu'impose l'article 8 est celui de la nécessité. Son analyse englobe notamment l'examen de la procédure de décision et d'exécution de chaque mesure de surveillance, et la façon dont les données ainsi obtenues sont utilisées. Ces garanties procédurales varieront en fonction de la nature et de l'intensité de l'ingérence. Elles devraient cependant prévenir efficacement les abus possibles. Dans son arrêt en l'affaire *Klass*, la Cour européenne des droits de l'homme a dit que : « Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne»[39]. Dans un arrêt ultérieur sur des mesures de surveillance, la Cour a indiqué que la loi devrait préciser « la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »[40].

35. Dans l'affaire *Roman Zakharov* évoquée ci-dessus, la Grande chambre de la Cour a ainsi résumé la jurisprudence de la Cour européenne des droits de l'homme sur la question de la nécessité d'une ingérence dans une société démocratique[41] :

> *[…] la Cour a reconnu que, lorsqu'elles mettent en balance l'intérêt de l'Etat défendeur à protéger la sécurité nationale au moyen de mesures de surveillance secrète, d'une part, et la gravité de l'ingérence dans l'exercice par un requérant du droit au respect de la vie privée, d'autre part, les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale. Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent. La Cour doit se convaincre de l'existence de garanties adéquates et effectives contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre. L'appréciation de cette question est fonction de toutes les circonstances de la cause, par exemple la nature, la portée et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit*

[37] Voir, par exemple, *Heglas c. République tchèque*, n° 5935/02, 1er mars 2007, paragraphe 74. La jurisprudence de la Cour européenne des droits de l'homme aborde également la question de l'accessibilité de la législation pour les personnes concernées, ce qui ne semble pas entrer ici en ligne de compte.
[38] *Roman Zakharov c. Russie* [GC], n° 47143/06, CrEDH 2015
[39] *Klass et autres c. Allemagne*, 6 septembre 1978, paragraphe 50, série A n° 28.
[40] Voir notamment *Prado Bugallo c. Espagne*, n° 58496/00, paragraphe 30, 18 février 2003; *Liberty et autres c. Royaume-Uni*, n° 58243/00, paragraphe 62, 1er juillet 2008.
[41] *Roman Zakharov*, paragraphe 232

interne. La Cour doit rechercher si les procédures de contrôle du déclenchement et de la mise en œuvre de mesures restrictives sont de nature à circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique ».

36. Dans l'affaire *Digital Rights Ireland and Seitlinger and Others* évoquée ci-dessus, la Cour de justice européenne a estimé en particulier que la Directive 2006/24 sur la conservation des données ne prévoyait pas de règles claires et précises sur la portée de l'ingérence, et n'exigeait pas de rapport entre les données conservées et la gravité de l'infraction ou de la menace à la sécurité publique. Elle a reproché à la directive de ne pas mettre en place de conditions matérielles ou procédurales (comme le contrôle préalable par une autorité administrative ou une juridiction) visant à limiter l'accès aux données conservées par les autorités nationales et leur utilisation. Elle a par ailleurs constaté que la directive ne fixait pas sur des critères objectifs la durée de conservation des données. Et qui plus est, elle ne contenait pas de garanties suffisantes permettant d'assurer la protection efficace des données conservées (paragraphes 56 et suivants).

37. On pourrait arguer que l'arrêt devrait être interprété comme interdisant totalement la conservation indifférenciée et générale de données. Même si l'on ne se range pas à une interprétation aussi radicale, il est clair que la conservation indifférenciée et générale de données est une source majeure d'inquiétude publique, que seul saurait pallier un robuste système de contrôle indépendant (voir également ci-dessous les paragraphes 98 et suivants et 112 et suivants).

B. Situations dans lesquelles les autorités publiques sont habilitées à procéder à une surveillance secrète et à collecter des métadonnées

38. Il convient tout d'abord d'examiner la clarté du champ d'application *matériel* des articles 19 et 20c, et la prévisibilité des situations dans lesquelles la police peut mettre en place une surveillance secrète ou obtenir des métadonnées[42].

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 l'analyse de proportionnalité que requiert l'article 8 de la Convention présente un volet matériel ; 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

[42] L'exigence de prévisibilité s'applique au champ d'application matériel de la loi, mais aussi aux garanties procédurales. Dans sa décision du 29 juin 2006 en l'affaire *Weber et Saravia c. Allemagne*, n° 54934/00, paragraphe 95, 29 juin 2006, la Cour européenne des droits de l'homme a formulé ainsi les « garanties minimales […] contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements ». Au niveau universel, les principes sont similaires : dans son rapport sur le contrôle des services de renseignement (intitulé *Compilation des bonnes pratiques concernant les cadres juridique et institutionnel et des mesures propres à garantir le respect des droits de l'homme par les services de renseignements dans le cadre de la lutte antiterroriste*) préparé à la demande du Conseil des droits de l'homme, le rapporteur spécial Martin Scheinin recommande (pratique n° 21) que le droit interne définisse : « le type de mesures de recherche de renseignements à la disposition des services secrets; les objectifs de la recherche de renseignements autorisés; les catégories de personnes et d'activités pouvant être visées par la recherche du renseignement; le niveau de suspicion requis pour justifier le recours à des mesures de recherche du renseignement; la durée maximum d'application desdites mesures; et la procédure d'autorisation, de contrôle et d'analyse du recours à ces mesures ».

(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[43].

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[44] 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*. La Commission de Venise rappelle qu'en l'affaire *Iordachi et autres c. Moldova*, la Cour européenne des droits de l'homme avait reproché à la législation nationale d'autoriser les écoutes téléphoniques dans les affaires portant sur plus de la moitié des infractions répertoriées dans le Code pénal[45].

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[46]. 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 (comme dans l'affaire *Lind c. Russie* devant la Cour européenne des droits de l'homme[47]). 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[48].

44. En l'affaire *Roman Zahkarov* évoquée ci-dessus, la Cour européenne des droits de l'homme avait souligné 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

[43] La loi ne qualifie en tout cas pas le but ni l'ampleur de la possession.

[44] Voir *Niemietz c. Allemagne*, 16 décembre 1992, paragraphes 27-33, série A n° 251-B

[45] *Iordachi et autres c. Moldova*, n° 25198/02, paragraphe 44, 10 février 2009

[46] Les autorités polonaises ont indiqué que le tribunal n'est pas astreint par le législateur à approuver la surveillance secrète, même si la demande est solidement étayée sur le fond et la forme. C'est une bonne chose, mais comme expliqué ci-dessous, la loi elle-même devrait décrire plus précisément les critères que doit appliquer le juge pour décider s'il doit ou non autoriser la surveillance dans une enquête pénale sur des faits figurant dans la liste du paragraphe 1 de l'article 19.

[47] *Lind c. Russie*, n° 25664/05, 6 décembre 2007, paragraphes 77 et 78; l'affaire *Lind* portait toutefois sur l'autorisation d'une détention préventive, et non pas d'une surveillance.

[48] L'exigence de soumission de preuves factuelles découle dans une certaine mesure du paragraphe 1a de l'article 19, qui veut que la police fournisse au tribunal les informations justifiant la nécessité du contrôle opérationnel.

mesures de surveillance secrète, comme par exemple des actes mettant en péril la sécurité nationale. Il 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 » (paragraphe 260). Bien sûr, le but même de la surveillance secrète est d'obtenir un complément d'éléments de preuve lorsque ceux que l'on possède déjà ne permettent pas de lancer des poursuites. 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[49].

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. L'utilité de l'information recherchée par la police est un autre aspect du principe plus général de proportionnalité évoqué ci-dessus. Là encore, il n'est pas indispensable que la police soit sûre du résultat : il suffit qu'elle démontre que la surveillance permettra *probablement* d'obtenir cette information. Mais une telle affirmation doit être étayée par certains faits et indices.

d. Subsidiarité

46. La dernière exigence que prévoit la loi est la *subsidiarité* (dernière phrase du paragraphe 1 de l'article 19) : la surveillance secrète ne peut être ordonnée que lorsque d'autres moyens paraissent inefficaces ou s'il est très probable qu'ils seront inefficaces ou inutiles. Là encore, cette exigence est indispensable à la proportionnalité de la mesure : la surveillance secrète doit être un instrument de dernier recours[50].

e. Valeur probante de l'information

47. Enfin, 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[51]. La CEDH ne traite pas, en règle générale, de l'admissibilité des éléments de preuve. Elle n'exige pas l'exclusion *inconditionnelle* de tout élément de preuve obtenu de façon irrégulière[52]. Une règle rigide d'exclusion en la matière est moins nécessaire lorsque la loi et les pratiques prévoient des contrôles suffisants de prévention des abus de pouvoirs d'investigation par la police ou les services de sécurité. La loi polonaise dit clairement que les renseignements obtenus sans l'autorisation préalable d'un tribunal (ou l'autorisation *a posteriori* exigée au paragraphe 3 de l'article 19 dans le cas d'une procédure d'urgence) ne sont pas admissibles dans les procédures pénales.

48. On ne sait toutefois 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

[49] Par « éléments de preuve », la Commission de Venise n'entend pas nécessairement les preuves obtenues, enregistrées et contrôlées selon les règles formelles de la procédure pénale.

[50] La Commission de Venise a par exemple trouvé une vérification similaire en trois étapes dans la législation danoise, qui autorise la surveillance lorsque : 1) il existe des motifs spécifiques de soupçonner que des informations sont transmises par ou à la cible de la surveillance ; 2) la mesure de coercition est strictement nécessaire à l'enquête ; 3) l'enquête porte sur une infraction passible de six ans d'emprisonnement ou plus, ou alors s'il s'agit d'enquêter à titre préventif sur certaines infractions figurant sur une liste, comme le terrorisme. Se reporter au rapport de 2015 préparé par l'Agence des droits fondamentaux de l'Union européenne *Etude de la FRA sur le cadre juridique des Etats membres en matière de surveillance* (non traduit, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Mapping Member States' legal frameworks*, p. 20).

[51] Si elles sont directement utilisables comme éléments de preuve, ou alors s'il est possible d'utiliser d'autres éléments de preuve obtenus *à la faveur* d'une surveillance illicite.

[52] A l'exception des preuves obtenues sous la torture, etc. ; voir par exemple *Harutyunyan c. Arménie*, n° 36549/03, paragraphes 58 et suivants, CrDEH 2007-III

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). Il convient donc de se demander si cette formulation répond à l'exigence de prévisibilité de la loi posée à l'article 8 de la CEDH[53].

50. Tout d'abord, contrairement à l'infraction déjà commise ou en train de se commettre, la prévention s'appuie sur une évaluation prospective. Bien sûr, la distinction n'est pas parfaitement claire, particulièrement en ce qui concerne les infractions envisagées mais non commises en général, et le terrorisme et le crime organisé en particulier. En tout cas, la marge d'incertitude liée à l'appréciation des événements futurs accroît les possibilités de détournement ou d'abus de ce mode d'investigation.

51. La Commission de Venise rappelle qu'en l'affaire *Szabó et Vissy c. Hongrie*[54], la Cour européenne des droits de l'homme avait dit que l'exigence de prévisibilité de la loi ne va pas jusqu'à imposer à l'Etat d'adopter des dispositions juridiques énumérant dans le détail toutes les situations pouvant conduire à la décision de mise en place d'une surveillance secrète. La mention de menaces terroristes ou d'opérations de sauvetage pouvait être considérée comme donnant en principe à la population les indications nécessaires. La Cour avait ensuite comparé la situation en Hongrie avec celle qu'elle avait observée en Moldova à propos de l'affaire *Iordachi et autres* évoquée précédemment. Dans ce dernier cas, elle avait critiqué le droit national parce qu'il autorisait la mise sur écoute dans un très grand nombre d'enquêtes pénales. Il convient donc d'examiner si cette même logique s'applique à la collecte de métadonnées.

52. Dans l'affaire *Uzun* évoquée ci-dessus (surveillance par GPS d'une voiture soupçonnée d'être utilisée par des terroristes), la Cour européenne des droits de l'homme avait tout d'abord examiné si la loi autorisant la mesure était prévisible. Tout en estimant qu'elle pouvait *s'inspirer* des principes applicables à la surveillance « classique » des télécommunications, elle avait reconnu que ces derniers n'étaient pas directement applicables à la surveillance par GPS, qui constitue une ingérence moindre dans la vie privée de la personne que l'interception de ses conversations téléphoniques (paragraphe 66).

53. La Cour n'avait pas conclu en l'affaire *Uzun* à la violation de l'article 8 de la CEDH en particulier parce que la surveillance par GPS « ne pouvait être ordonnée qu'à l'égard d'une personne soupçonnée d'une infraction extrêmement grave » (paragraphe 70). En d'autres termes, la loi allemande restreignait le recours à cette technique aux cas les plus graves. L'article 20c de la loi sur la police ne le fait pas : elle 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)[55].

---

[53] La Commission de Venise estime que la formule « missions de recherche et de sauvetage » décrit avec une précision suffisante des situations dans lesquelles la police est habilitée à collecter des métadonnées.

[54] N° 37138/14, paragraphe 64, 12 janvier 2016 (non encore définitif)

[55] Dans l'affaire *Uzun*, la surveillance par GPS avait duré environ trois mois ; la loi ne prévoit aucune limitation de la durée de collecte de métadonnées en vertu de l'article 20c.

54. Dans son rapport de 2015 sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique[56], la Commission de Venise estimait qu'il « existe un lien étroit entre la manière plus ou moins précise dont le mandat du service est défini et le risque d'abus ». 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[57].

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

55. Il convient maintenant de s'interroger sur la *probabilité*, dûment étayée par des faits pertinents, sur laquelle doit s'appuyer la collecte de métadonnées. C'est une question délicate, notamment du fait que la collecte de métadonnées, contrairement à la surveillance classique, n'est souvent pas « ciblée » (voir aux paragraphes 66 et suivants l'analyse de la collecte non ciblée d'informations). Il n'est donc pas toujours possible de lier la collecte de métadonnées à une personne ou à un groupe soupçonnés d'une infraction particulière.

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[58].

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 collecte de métadonnées aide très utilement à reconstituer une chaîne de contacts, c'est-à-dire à identifier les réseaux d'un suspect, ce qui veut dire qu'il y est souvent recouru relativement tôt dans une enquête. Mais le principe général de proportionnalité s'applique aussi à elle, comme à toute mesure de coercition, et il convient toujours d'arbitrer au mieux entre l'efficacité et l'ingérence dans la vie privée. 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. Les garanties procédurales susceptibles de prévenir de tels abus seront abordées aux paragraphes 110 et suivants.

---

[56] CDL-AD(2015)011, paragraphe 70.

[57] La Commission de Venise croit comprendre que les pouvoirs conférés à d'autres services de l'Etat en matière de collecte de métadonnées sont délimités en fonction de leurs missions respectives.

[58] Le niveau de probabilité renvoie dans une certaine mesure aux critères analysés précédemment à propos de la surveillance classique : nécessité de justification matérielle, minimum de probabilité d'obtention d'informations importantes, etc.

59. La loi devrait par ailleurs contenir une règle indiquant sur le plan matériel à la police quand elle peut recourir à cette méthode. Comme il a été dit au paragraphe 58, 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 (se reporter au document CDL-REF(2016)036). Il revient aux spécialistes des domaines concernés de dire si les termes techniques qui y figurent décrivent les métadonnées avec une précision suffisante. Un certain nombre de choses n'en frappent pas moins l'attention du non-spécialiste.

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[59]. 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. La Commission de Venise a dit dans son rapport de 2015 que « la jurisprudence, même lorsqu'elle formule des règles détaillées et émane de la Cour suprême ou constitutionnelle, n'est pas plus suffisante en elle-même – pour réglementer [la surveillance secrète] – qu'une législation secondaire »[60].

[59] Le document d'information du 29 avril 2016 remis aux rapporteurs à la réunion qui a lieu à la chancellerie du Comité des ministres dit au paragraphe 5 que les métadonnées n'englobent pas les identifiants et mots de passe, ni non plus les adresses des sites Internet consultés. Pourtant, d'autres interlocuteurs avec lesquels les rapporteurs se sont entretenus à Varsovie voyaient les choses autrement. De plus, l'information reçue du ministère de l'Intérieur polonais donnait à comprendre que la police peut collecter des informations de ce type dans le cadre de la surveillance des métadonnées ; le matériel statistique sur la collecte de métadonnées contenait d'ailleurs des entrées comme « adresses www » et « chats », qui se rapportent clairement au contenu.

[60] Voir CDL-AD(2015)011, paragraphe 93. Il n'est toutefois pas exclu que des textes législatifs secondaires traitent d'aspects très techniques ou très secrets de la collecte 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 [61] offerts au public peut, moyennant le consentement de l'utilisateur s'il s'agit d'une personne physique, traiter *d'autres données* [c'est nous qui soulignons] 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 et habilite la personne elle-même à décider de la mesure dans laquelle elle accepte de partager des informations à caractère personnel avec tel ou tel acteur.

64. La Commission de Venise reconnaît que le rapide progrès technique actuel impose une certaine souplesse dans la réglementation de la collecte des métadonnées. Mais les services gouvernementaux ne devraient pas pouvoir élargir la notion de métadonnées au-delà de son sens originel pour lui faire couvrir des types d'informations complètement nouveaux. Si le besoin se fait sentir de réglementer l'accès à de nouvelles catégories d'informations et d'introduire de nouvelles formes de surveillance, seul le législateur devrait avoir compétence pour définir les données qu'il est possible de collecter, avec les motifs admissibles et les procédures afférentes.

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

66. La surveillance secrète « classique » permet d'obtenir des informations sur une personne, un groupe ou une organisation. Mais les mesures modernes de surveillance, en particulier la collecte de métadonnées, débutent parfois sans cible spécifique. Le ciblage n'est déterminé *qu'après* collecte et filtrage des données ainsi obtenues.

67. En « vidant » par exemple un relais de téléphonie mobile, on peut savoir quels téléphones portables étaient présents dans une zone à un moment donné, ce qui aidera la police à savoir par exemple si les téléphones portables de membres connus d'une organisation criminelle se trouvaient dans la zone au moment du cambriolage d'une banque. Cette technique peut aussi permettre d'identifier qui se trouvait dans la zone d'une grande manifestation contre le gouvernement. On voit aisément l'effet dissuasif que cela peut avoir sur l'exercice des libertés d'association et de réunion protégées par l'article 11 de la CEDH. « Cette caractéristique explique la valeur [que cette forme de surveillance] peut revêtir au regard des opérations de

[61] TIC (technologies de l'information et de la communication) désigne d'une façon générale tous les matériels et applications de communication utilisés en radio, télévision, téléphonie portable, informatique et réseaux, systèmes par satellites, etc., de même que les services et applications associés, comme vidéoconférences et enseignement à distance.

sécurité, mais aussi les risques [qu'elle] peut comporter pour les droits individuels. »[62] Même lorsque cette surveillance non ciblée est utilisée à des fins légitimes (par exemple pour prévenir une attaque terroriste, ou dans une opération de recherche et de sauvetage) et revient moins cher que d'autres méthodes, elle touche inévitablement un grand nombre de personnes innocentes ou étrangères à l'affaire.

68. Il convient de commencer par se demander si la loi sur la police autorise la surveillance à très large ciblage. Le paragraphe 7 de son article 19 impose à la police d'indiquer « les données d'une personne ou autres données permettant de déterminer sans ambiguïté l'entité ou l'objet de la surveillance ». On ne sait pas très bien dans quelle mesure le terme d'objet de la surveillance peut désigner un groupe nombreux de personnes (les habitants d'un quartier, par exemple, ou un groupe de manifestants ou de fidèles dans une église). La formulation « déterminer sans ambiguïté », interprétée au sens strict, garantit qu'il n'est pas possible de s'appuyer sur l'article 19 pour ordonner une surveillance sans aucune individualisation[63], même si elle porte sur un groupe de personnes. Les surveillances « classiques » de la police polonaise devraient donc toujours être ciblées[64].

69. Pour ce qui est de la collecte de métadonnées (article 20c), en revanche, rien dans la loi ne semble s'opposer à ce que la police en collecte sans ciblage. La Commission de Venise rappelle dans ce contexte que l'Assemblée parlementaire du Conseil de l'Europe a invité dans sa résolution 2045 (2015)[65] les Etats membres « à veiller à ce que leur droit interne autorise la collecte et l'analyse des données à caractère personnel (métadonnées comprises) uniquement […] à la suite d'une décision de justice rendue sur la base de motifs raisonnables de soupçonner la cible de prendre part à des activités criminelles ».

70. La Commission de Venise serait encline à se montrer moins catégorique. L'Assemblée semble mettre en question le principe même de la surveillance stratégique, qui ne se fonde pas sur une décision de justice ciblée. La jurisprudence de la Cour européenne des droits de l'homme semble quant à elle admettre un ciblage large de collecte d'informations[66]. 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[67].

---

[62] Rapport de 2015, CDL-AD(2015)011, paragraphe 3

[63] Par individualisation, la Commission de Venise ne veut pas dire que la police doit toujours connaître exactement l'identité de la personne placée sous surveillance ; parfois, un mandat de surveillance peut porter sur l'utilisateur anonyme d'une ligne téléphonique ou d'un ordinateur suspect, etc.

[64] Les autorités polonaises ont confirmé dans leur communication écrite que la loi sur la police ne permet pas de demander la surveillance secrète d'un groupe indéfini ou d'une personne anonyme : il devrait toujours s'agir d'une personne ou d'un terminal de télécommunications bien défini.

[65] Résolution *Les opérations de surveillance massive*, adoptée le 21 avril 2015, paragraphe 19.1.

[66] Dans l'affaire *Weber et Saravia c. Allemagne* évoquée précédemment, par exemple, la Cour européenne des droits de l'homme analysait le système de surveillance stratégique employé en Allemagne (interception non ciblée de communications et analyse de leur contenu par mots clés) et avait conclu à sa compatibilité avec l'article 8 de la CEDH.

[67] Dans *Weber et Saravia*, paragraphes 96 et 97, la Cour européenne des droits de l'homme insistait sur le fait que dans le système allemand, la loi « énumérait très précisément […] les infractions pour la prévention desquelles l'interception stratégique de télécommunications pouvait être ordonnée ». Elle « définissait donc de façon claire et précise les infractions pouvant donner lieu à un mandat d'interception ». Elle « indiquait les catégories de personnes susceptibles de faire l'objet d'écoutes téléphoniques » et « les intéressés devaient de surcroît avoir employé des mots clés de nature à déclencher une enquête sur les dangers » énumérés dans la loi, « ou être des ressortissants étrangers ou des sociétés étrangères ».

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[68]. 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[69]. En ce qui concerne les exigences définies au paragraphe 2 de l'article 8 de la CEDH, 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 »)[70].

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[71].

---

[68] Voir *Roman Zakharov*, cité précédemment, paragraphe 275

[69] Voir Rapport de 2015, paragraphe 98

[70] Ce qui vient d'être dit ne s'applique pas à la surveillance à ciblage large, qui englobe nécessairement une grande majorité de personnes parfaitement innocentes qui n'ont rien à voir avec l'objet de l'enquête. Comme on l'a vu plus haut (paragraphes 66 et suivants), ce type de surveillance peut être admissible pour autant qu'un dispositif efficace de contrôle soit en place.

[71] Les autorités polonaises ont expliqué à la Commission de Venise qu'il appartient en fin de compte au juge chargé de l'affaire de décider de l'admissibilité des éléments de preuve obtenus par surveillance secrète. S'il en est ainsi, la loi devrait le dire clairement ; de plus, elle devrait préciser les circonstances dans lesquelles le juge peut déclarer inadmissibles des informations obtenues par la surveillance.

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

75. L'article 19 de la loi sur la police indique ce qu'il convient de faire de l'information couverte par le secret professionnel. Les membres compétents de la police doivent :

- détruire l'information si elle bénéficie de la protection du secret professionnel *absolu* auquel ont droit les avocats et les prêtres (article 19, paragraphe 15f, alinéa 1, de la loi, lu en combinaison avec l'article 178 du Code de procédure pénale polonais)[72], ou ;
- transmettre l'information au procureur puis au tribunal, qui décidera ce qu'il convient d'en faire si ladite information jouit d'une protection *moins totale* du secret professionnel, comme dans le cas des notaires, des avocats et des conseillers juridiques (sauf il s'agit d'un avocat de la défense), de conseillers fiscaux, de médecins, de médiateurs ou de journalistes (article 19, paragraphes 15f, alinéa 2, et 15g à j de la loi, lu en combinaison avec l'article 178a et l'article 180, paragraphes 2 et 3, du Code de procédure pénale polonais).

76. La Commission de Venise observe tout d'abord que le secret de la communication entre l'avocat et son client est protégé non seulement par l'article 8 de la Convention (comme toute autre communication à caractère privé), mais implicitement aussi par son article 6, paragraphe 3, alinéa c. Le sceau de la confession est quant à lui protégé par l'article 9 de la Convention. On peut dire que ces deux formes de communication ont un statut particulier, même au regard de l'article 8 de la Convention ; en ce qui concerne le secret de la communication entre l'avocat et son client, du moins, la Cour européenne des droits de l'homme a estimé qu'il mérite une protection spéciale, du fait que « dans le cas d'un avocat, pareille intrusion peut se répercuter sur la bonne administration de la justice et, partant, sur les droits garantis par l'article 6 de la Convention »[73].

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 »[74], 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,

[72] L'article 178 dit qu'il n'est pas permis d'interroger en qualité de témoin 1) un avocat de la défense ou un avocat intervenant au titre de l'article 245, paragraphe 1, sur ce qu'il a appris dans son rôle de conseil juridique ou en s'occupant de l'affaire ; 2) un membre du clergé sur ce qu'il a appris en confession.

[73] *Smirnov c. Russie*, n° 71362/01, paragraphe 48, 7 juin 2007, avec autres références.

[74] La théorie des fruits de l'arbre empoisonné dit que les éléments de preuve provenant d'informations obtenues en violation de la loi doivent aussi être déclarés inadmissibles. Pour une analyse plus détaillée, voir Cour européenne des droits de l'homme, affaire *Gäfgen c. Allemagne* [GC], *n°* 22978/05, CrEDH 2010.

etc.). L'écoute de ces communications devrait en principe être interdite[75]. Aux Pays-Bas, par exemple, une discussion est en cours sur la possibilité que les cabinets d'avocats déposent au ministère de l'Intérieur une liste de lignes couvertes par le secret professionnel, et que ces numéros soient automatiquement exemptés de toute forme de surveillance.

80. La présomption ci-dessus n'est pas absolue. Dans sa jurisprudence, la Cour européenne des droits de l'homme indique que la Convention n'exige pas des Etats membres qu'ils ne surveillent jamais les communications entre un détenu et son avocat[76]. 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)[77].

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.

83. Cela est particulièrement important si la cible est un journaliste, car on peut ainsi connaître ses sources. La Commission de Venise rappelle que la protection des sources journalistiques constitue l'une des pierres angulaires de la liberté de la presse. Comme il ressort de l'affaire *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*[78], la Cour européenne des droits de l'homme soumet les ordonnances de divulgation pouvant conduire à l'identification des sources journalistiques à un contrôle extrêmement strict. Il devrait donc exister une quelconque procédure interne renforcée de décision lorsque la liberté de la presse est en jeu. Dans son rapport de 2015 évoqué ci-dessus, la Commission de Venise indiquait que « des méthodes devraient être élaborées afin de conférer aux avocats, journalistes et autres communicants privilégiés une certaine protection, sous la forme par exemple d'un seuil élevé ou très élevé en matière d'approbation d'opérations de collecte contre les intéressés, seuil auquel viendraient s'ajouter des garanties procédurales et un contrôle externe strict » (paragraphe 18).

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*. Dans l'affaire *Weber et Saravia* évoquée précédemment, le journaliste se plaignait que ses communications et ses sources pouvaient être divulguées en

[75] La Commission de Venise note à ce propos que l'article 15, paragraphe 1 (4a) de la loi permet à la police d'enregistrer des conversations « dans les pièces où sont accueillies les personnes arrêtées » ; cette interception ne serait pas soumise au régime général mis en place au paragraphe 1 de l'article 19. De plus, le paragraphe 6 (2) de ce même article permet à la police d'obtenir et d'enregistrer des images et des sons de personnes dans des pièces, ce qui peut être interprété comme une autorisation d'écoute dans des parloirs.

[76] *Erdem c. Allemagne*, n° 38321/97, paragraphe 65, CrEDH 2001-VII (extraits).

[77] *Erdem*, évoquée précédemment, paragraphe 67

[78] Evoqué précédemment, paragraphe 127

raison de la surveillance stratégique à laquelle se livrait le Service fédéral de renseignement. En l'espèce, la Cour européenne des droits de l'homme avait estimé que les garanties mises en place par l'Allemagne étaient suffisantes et minimisaient efficacement dans toute la mesure possible la divulgation des sources journalistiques, ce qui satisfaisait aux exigences de l'article 8 de la CEDH (paragraphe 151).

85. En conclusion, 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.

86. Toute norme matérielle régissant l'accès aux communications professionnelles des avocats resterait lettre morte sans un dispositif convenable de contrôle. La Commission de Venise aborde à la section D (en particulier aux paragraphes 91 et suivants et 112 et suivants) quelques dispositifs procéduraux de contrôle de la police et d'autres services, ainsi que de vérification de la légalité des opérations de surveillance. Le législateur national pourrait en particulier mettre en place un dispositif permettant d'empêcher la police de connaître les informations protégées par le secret professionnel – comme dans le système néerlandais décrit en l'affaire *Mulders c. Pays-Bas*, ou les règles de saisie de documents d'un avocat analysées dans l'affaire *Tamosius c. Royaume-Uni* (déc.) ; cf. *Wieser et Bicos Beteiligungen GmbH c. Autriche*[79].

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[80].

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[81]. 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.

---

[79] *Mulders c. Pays-Bas*, n° 23231/94, décision de la Commission du 6 avril 1995; *Tamosius c. Royaume-Uni* (déc.), n° 62002/00, CrEDH 2002-VIII; *Wieser et Bicos Beteiligungen GmbH c. Autriche*, n° 74336/01, CrEDH 2007-XI.

[80] Cette interprétation des paragraphes 8 et 9 de l'article 19 est confirmée par une synthèse de la loi préparée le 29 avril 2016 par la chancellerie du Comité des ministres de Pologne (page 4).

[81] Il ressort d'explications données par les autorités polonaises que la durée de conservation des données n'est pas fixe mais dépend de leur utilité dans la procédure. Les données doivent être détruites sans retard si elles ne contiennent pas d'éléments de preuve susceptible de justifier l'ouverture d'une affaire pénale, ou utiles dans une affaire pénale en instance.

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

89. La Commission de Venise reconnaît que la loi ne peut entièrement éviter les formulations à caractère général pour décrire les situations nécessitant une surveillance. Une loi quelque peu imprécise n'en peut pas moins être corrigée par des garanties procédurales (qui pallient le risque d'abus que suscite l'imprécision). Il est donc important de faire en sorte que l'organe chargé de faire respecter les règles soit professionnel, indépendant, et armé de tous les instruments juridiques nécessaires à l'accomplissement de sa mission de contrôle.

90. La Commission de Venise a estimé dans son rapport de 2015 (paragraphe 105) qu'il « semble que les deux garanties les plus importantes soient le processus d'autorisation (de la collecte et de l'accès aux données collectées) et le processus de suivi (contrôle). Il ressort nettement de la jurisprudence de la Cour [européenne des droits de l'homme] que ce dernier processus doit être confié à un organe indépendant et extérieur. La question qui se pose en l'occurrence est de savoir si le processus d'autorisation devrait lui aussi être 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. La Cour européenne des droits de l'homme ne considère pas l'autorisation juridictionnelle comme une condition *sine qua non*[82] pour une surveillance, mais elle y voit une importante garantie procédurale[83]. Le dispositif que met en place le paragraphe 1 de l'article 19 de la loi est donc bienvenu. De plus, 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 (cf. paragraphe 26).

93. La dérogation prévue au paragraphe 3 de l'article 19 pour les cas d'urgence se retrouve dans d'autres juridictions. En Lettonie, par exemple, la surveillance peut être lancée sans l'autorisation d'un magistrat s'il convient d'agir sans retard pour contrer un danger menaçant un intérêt public vital (actes terroristes, activités subversives, meurtre ou autre crime grave) ou en cas de menace directe à la vie, à la santé ou aux biens d'une personne. Un procureur doit alors être averti dans les 24 heures, et l'autorisation d'un magistrat obtenue dans les 72 heures[84]. La Commission de Venise observe qu'en Pologne, la dérogation pour 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[85]. Il conviendrait de reprendre ce point[86].

---

[82] *Kennedy c. Royaume-Uni*, n° 26839/05, 18 mai 2010

[83] Voir l'affaire *Association pour l'intégration européenne et les droits de l'homme et Ekimdjev c. Bulgarie*, n° 62540/00, paragraphes 81 et 84, 28 juin 2007, dans laquelle la Cour avait approuvé le système d'autorisation juridictionnelle des surveillances secrètes. Voir également l'arrêt en l'affaire *Klass et autres c. Allemagne*, évoquée précédemment, paragraphe 55, dans lequel la Cour européenne des droits de l'homme avait dit que la prééminence du droit « implique, entre autres, qu'une ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire, car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière ».

[84] Voir rapport de la the FRA, p. 54

[85] Les autorités polonaises ont assuré à la Commission de Venise que la possibilité de recourir à la surveillance secrète de courte durée, de deux ou trois jours par exemple, n'est pas autorisée sans contrôle. S'il en est ainsi, la loi devrait le préciser clairement.

94. L'autorisation juridictionnelle de la surveillance est une utile garantie contre l'abus, mais deux choses peuvent enrayer ce dispositif juridique. La première est le risque que les demandes surchargent les magistrats. Le contrôle juridictionnel de la surveillance devrait être considéré comme un aspect essentiel du travail du juge, et compté dans les statistiques judiciaires. Le juge devrait par ailleurs bénéficier de l'appui convenable de membres de son personnel possédant une connaissance suffisante des technologies et pratiques de surveillance. Faute de quoi, il sera tenté de se faciliter la tâche en se bornant à un contrôle de pure forme.

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. On comprend que « la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne »[87]. 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[88].

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[89]. Sa fonction serait de défendre les intérêts de la personne ciblée par la surveillance [90].

ii. Contrôle rétrospectif

98. Il y a plusieurs autres façons de remédier aux insuffisances de la procédure d'autorisation. 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

---

[86] Voir *Roman Zakharov*, cité précédemment, paragraphe 266 : « Le droit interne ne restreint pas l'utilisation de la procédure d'urgence aux cas impliquant un péril grave et imminent pour la sécurité nationale, militaire, économique ou écologique du pays ; il laisse aux autorités une latitude illimitée 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 (voir, a contrario, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, paragraphe 16). »

[87] *Roman Zakharov c. Russie*, citée précédemment, paragraphe 233. Voir également *Klass et autres c. Allemagne*, cité précédemment, paragraphes 55 and 56.

[88] En l'affaire *Dumitru Popescu c. Roumanie (n° 2)*, n° 71525/01, 26 avril 2007, paragraphe 78, la Cour avait estimé que l'autorité roumaine qui avait autorisé la surveillance (à savoir le procureur) n'était pas indépendante de l'exécutif. Les rapporteurs ont été informés qu'un bureau du procureur spécial récemment créé est chargé de suivre plus étroitement les activités d'investigation des services de sécurité et de renseignement. C'est également une bonne chose, qui ne constitue toutefois pas à une garantie procédurale suffisante, pour les raisons indiquées.

[89] Voir une description de la fonction de l'avocat du Royaume-Uni, Rapport de 2007, paragraphes 215 et 216.

[90] La participation de l'avocat de la vie privée peut revêtir diverses formes. En Autriche, par exemple, le Commissaire à la protection judiciaire (*Rechtsschutzbeauftragter*, RSB) assure un niveau de protection supplémentaire aux personnes soumises à leur insu à des enquêtes secrètes. Il approuve les enquêtes secrètes (*verdeckte Ermittlung*) ou les enregistrements audio et vidéo secrets réalisés dans le contexte de l'observation de groupes soupçonnés de menacer gravement la sécurité publique par des actes de violence à motivation religieuse ou idéologique. Le ministre fédéral de l'Intérieur consulte le Commissaire pendant les analyses opérationnelles et stratégiques de données à caractère personnel. Les analyses de ce type s'inscrivent dans la défense contre les organisations criminelles ou la prévention des dangers résultant de la préparation ou de la commission d'infractions pénales. Le Commissaire émet un avis sur chaque surveillance ; l'analyse peut ensuite avoir lieu (rapport de la FRA, p. 53).

fond donnerait à l'accusé, du moins en théorie, l'occasion de contester la légalité de sa surveillance[91]. Mais plusieurs autres questions se posent encore.

99. Tout d'abord, si la contestation est possible, son seul effet pour l'accusé serait de rendre inadmissibles les éléments de preuve obtenus par surveillance. Autrement dit, elle ne servirait de rien si, par exemple, l'accusé demande une indemnisation pour l'ingérence qu'il affirme illicite dans sa vie privée. De plus, ce recours ne serait accessible qu'à l'accusé, mais pas à une tierce personne affectée dans sa vie privée par l'interception illicite – du simple fait que sa situation ne lui permettrait pas de demander l'exclusion d'éléments de preuve.

100. Deuxièmement, on ne voit pas clairement si la juridiction contrôlant la validité de l'ordre du juge autorisant la surveillance dans la procédure sur le fond aurait pleine compétence en la matière, ni si l'accusé aurait accès à la totalité des informations qui avaient justifié la surveillance. Il semble aux rapporteurs qu'en Pologne, les informations de « contrôle opérationnel » sont en général tenues secrètes[92]. 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[93]. 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[94].

101. Le point le plus important, enfin : 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. Dans le cas de la surveillance « classique », de nombreux pays exigent que la personne ciblée soit normalement *notifiée*, bien sûr après coup, du fait qu'elle a été surveillée et des motifs de la surveillance (si la notification ne risque pas de compromettre des méthodes d'investigation ou des sources)[95]. 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. C'est pourquoi la notification de la personne ciblée n'est pas une exigence absolue, et les autorités peuvent ne pas s'y soumettre dans certains cas légitimes. 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

[91] On ne sait pas très bien si le tribunal examinant l'affaire sur le fond pourra contrôler et annuler la décision du tribunal qui a autorisé la surveillance. Il a été dit aux rapporteurs que les récents changements apportés au Code de procédure pénale, et qui ne font pas l'objet du présent avis, réduisent sensiblement la capacité du tribunal à déclarer inadmissibles des éléments de preuve obtenus illégalement.

[92] Ce qui est confirmé, dans une certaine mesure, par le paragraphe 16 de l'article 19, qui dit que les informations collectées par contrôle opérationnel ne sont pas communiquées à la personne qui en a fait l'objet. De plus, l'article 20b de la loi dit que la communication d'informations relatives à la forme détaillée, aux principes et à l'organisation de l'enquête préliminaire, des activités menées ainsi que des mesures prises et de leurs modes de mise en œuvre n'est autorisée qu'en cas de soupçon justifié qu'une infraction poursuivie à la suite d'une inculpation était liée à ces activités ; en d'autres termes, dans des affaires mineures de demandes injustifiées de surveillance ne constituant pas un comportement réprimé par le droit pénal, les informations qui ont justifié la surveillance peuvent être considérées comme confidentielles puisqu'il est possible de prétendre qu'elles contiennent des éléments liés à l'organisation de l'enquête préliminaire, etc.

[93] Voir *Mirilashvili c. Russie*, n° 6293/04, paragraphes 200 et suivants, 11 décembre 2008 ; *Roman Zakharov*, cité précédemment, paragraphe 261

[94] Les autorités polonaises ont expliqué que les dispositions figurant aux paragraphes 1 et 4 de l'article 156 du Code de procédure pénale polonais garantissent aux parties dans la procédure judiciaire plein accès au dossier de l'affaire, et même aux informations classifiées.

[95] Voir le Rapport de 2015, paragraphes 39 et 126

de la surveillance *de novo*[96]. 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)[97].

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[98]. 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[99].

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)[100], et à engager toutes les actions récursoires appropriées en l'espèce[101].

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[102]. 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

---

[96] Il n'y a pas qu'aux tribunaux que puisse être confié l'examen de ces plaintes ; les Etats ont toute latitude pour mettre en place d'autres dispositifs de contrôle et d'examen des plaintes du moment qu'ils sont efficaces : médiateurs, commission nationale des droits de l'homme, bureau national d'audit, organe de surveillance parlementaire, inspection générale, organe spécialisé de contrôle des activités de renseignement et commission d'examen des plaintes concernant les services de renseignement (pour des exemples de dispositifs nationaux, voir le rapport des Nations unies sur le contrôle des services de renseignement, p. 11). La Commission de Venise juge toutefois que l'examen judiciaire ou quasi judiciaire des plaintes fournit des garanties plus solides.

[97] Le paragraphe 14 de l'article 19 confie au procureur le contrôle de la surveillance secrète.

[98] Contrairement à un dispositif d'examen des plaintes, un tel organe vérifierait régulièrement d'office les opérations de surveillance, et non pas nécessairement à la demande des personnes ciblées.

[99] Le rapport des Nations unies sur le contrôle des services de renseignement cité précédemment indique à ce sujet qu'un système efficace de contrôle des activités de renseignement englobe au moins un organisme civil indépendant des services de renseignement et de l'exécutif (pratique 6).

[100] Le Commissaire aux droits de l'homme du Conseil de l'Europe, dans son document thématique de 2015 intitulé *La surveillance démocratique et effective des services de sécurité nationale*, disait au paragraphe 14 qu'il convient de « garantir que l'ensemble des organes chargés de contrôler les services de sécurité ont accès à toutes les informations qu'ils jugent nécessaires, quel que soit leur niveau de classification, pour s'acquitter de leur mandat. L'accès aux informations des organes de contrôle doit être inscrit dans la loi et garanti par le recours aux pouvoirs et outils d'investigation qui assurent cet accès. Il faut interdire sous peine de sanctions toute tentative de restreindre l'accès des organes de contrôle à des informations classifiées. »

[101] La Commission de Venise se borne à décrire les pouvoirs de l'organe indépendant de contrôle chargé de la vérification de la légalité et de la nécessité des surveillances. Mais le mandat de cet organe peut-être plus large, et comprendre des compétences portant sur le contrôle plus stratégique des activités des services concernés de l'Etat. On pourrait par exemple explorer l'idée d'associer un tel organe à l'attribution par le Parlement des budgets de surveillance ; en lui confiant cette compétence, la loi pourrait lui mettre en main un outil additionnel très efficace de lutte contre les demandes abusives de surveillance.

[102] Aux dires des autorités polonaises, le Tribunal constitutionnel polonais avait estimé que le contrôle juridictionnel des activités opérationnelles constitue la meilleure solution (section 5.2.5 de l'arrêt).

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. Pour conclure, 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[103]. 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. Cette dernière (tout comme les services de sauvetage) a très souvent besoin de ce type de données, et la mise en place d'un système d'autorisation préalable indépendante n'est ni réaliste ni nécessaire – du moins en ce qui concerne les métadonnées moins sensibles (comme les informations relatives à l'abonnement). En pareil cas, il suffirait de notifier postérieurement la juridiction (ou un organe de contrôle indépendant – voir paragraphe 114).

[103] Dans l'affaire *Weber et Saravia*, la Cour européenne des droits de l'homme avait jugé acceptable le système allemand de contrôle des surveillances stratégiques (non ciblées), constitué d'un comité parlementaire de contrôle composé de neuf membres du Parlement (dont des représentants de l'opposition), du ministre fédéral et d'une commission indépendante chargée d'autoriser les mesures de surveillance et dotée de pouvoirs notables à toutes les étapes de l'interception. Dans l'affaire *Kennedy c. Royaume-Uni*, citée précédemment, la Cour européenne des droits de l'homme avait approuvé un système dans lequel un organe indépendant, la Commission des pouvoirs d'enquête (*Investigatory Powers Tribunal,* IPT), formée de personnes qui occupaient ou avaient occupé de hautes fonctions judiciaires et des juristes chevronnés, était habilité à annuler des mandats d'interception, travaillait avec le Commissaire chargé des interceptions de communications *(Interception of Communications Commissioner)*, 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 (voir également *Telegraaf Media*, cité précédemment, paragraphe 98).

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[104].

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. Certains pays remettent cette fonction au procureur, qui est un peu moins directement lié aux enquêtes de la police. En théorie, la culture du parquet serait plus dominée par la loi que celle de la police, mais le degré d'indépendance formelle et institutionnelle du ministère public par rapport à l'exécutif varie d'un pays à l'autre[105]. Et comme on l'a vu, la Cour européenne des droits de l'homme a tendance à ne pas considérer le procureur comme un magistrat « indépendant » auquel confier le contrôle des opérations de police[106].

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[107].

116. Il vaudrait mieux recourir à des organismes composés d'experts pour compléter ou remplacer le contrôle juridictionnel. Dans son rapport de 2007 (paragraphes 218 et suivants), la Commission de Venise décrit la composition et le mandat d'organes de ce type ; elle dit que « lorsqu'un groupe d'experts n'opère que comme un substitut aux autorisations judiciaires et

---

[104] A savoir : 1) nombre de cas d'obtention de données de télécommunications et de communications postales ou en ligne au cours de la période, avec types de données ; 2) caractérisation juridiques, avec objet auxquels se rapportaient les demandes de données de télécommunications et de communications postales ou en ligne, ou informations sur l'obtention de données visant à sauver des vies humaines et à préserver la santé ou destinées à des missions de recherche et de sauvetage.

[105] Voir CDL-AD(2010)040, *Rapport de la Commission de Venise sur les normes européennes relatives à l'indépendance du système judiciaire : partie II - le ministère public*, paragraphes 23 et suivants.

[106] Voir *Dumitru Popescu c. Roumanie (n° 2)*, citée précédemment ; *Iordachi et autres*, citée précédemment, paragraphe 47 ; *Roman Zakharov*, paragraphes 277 et suivants.

[107] Voir Rapport de 2007 (paragraphes 201 et suivants), dans lequel la Commission de Venise arrivait à la conclusion que « les tribunaux de droit commun ne semblent pas être le meilleur instrument de contrôle des agences de sécurité et de renseignement ou de réparation de leurs agissements » (paragraphe 217).

non pas comme un complément, il est très important que ce groupe soit suffisamment compétent et indépendant pour exercer un contrôle effectif » (paragraphe 240).

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[108]. 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)[109].

118. La Commission de Venise répète que l'existence d'un contrôle rétrospectif n'exclut pas la possibilité d'une autorisation préalable juridictionnelle pour certaines des mesures de surveillance les plus lourdes, y compris pour ce qui est de la collecte de métadonnées. Dans certains pays (comme la Suède), le contrôle juridictionnel préalable est complété par un contrôle rétrospectif confié à un organe indépendant. L'expérience d'autres pays révèle que cela n'érode pas l'indépendance de la justice. Un tel organe présente le gros avantage de pouvoir être chargé d'une mission spéciale de surveillance de la collecte de métadonnées (et ainsi de prévention des abus) dans des situations controversées : communications couvertes par le secret professionnel, ciblage géographique, métadonnées se rapportant au contenu, consultation préventive de métadonnées (en cas de menace à la vie ou à la sécurité), etc.

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.

121. Dans l'affaire *Roman Zakharov* évoquée ci-dessus, la Cour européenne des droits de l'homme disait (paragraphe 270) « qu'un système tel que le système russe, qui permet […] à la police d'intercepter directement les communications de n'importe quel citoyen sans […] obligation de présenter une autorisation d'interception au fournisseur de services de communication ou à quiconque, est particulièrement exposé aux abus. La nécessité de disposer de garanties contre l'arbitraire et les abus apparaît donc particulièrement forte. » Cet accès direct n'est ainsi pas interdit en soi par la Cour européenne des droits de l'homme ; mais

[108] Dans l'affaire *Klass et autres* citée précédemment, au paragraphe 56, la Cour européenne des droits de l'homme a estimé en principe souhaitable que le contrôle soit confié à un juge, mais constaté que l'exclusion du contrôle judiciaire peut être compatible avec la Convention, du moment que l'organe de contrôle est indépendant des autorités effectuant la surveillance et possède des compétences et pouvoirs suffisants pour procéder en permanence à un contrôle efficace.

[109] Selon le rapport de 2015 de la FRA, les organes parlementaires de contrôle de plusieurs membres de l'UE (Croatie, Hongrie, Lituanie et Roumanie) examinent également les plaintes. Les organes de contrôle autres que des commissions parlementaires, comme ceux qui assurent le contrôle exécutif et technique, peuvent aussi constituer une voie de recours, comme en Belgique, en Croatie, en Allemagne, au Danemark, en Hongrie, à Malte, aux Pays-Bas, au Portugal et en Suède (p. 70).

comme il ouvre grand la porte aux abus, tout Etat qui s'en dote doit prévoir des garanties particulièrement solides.

122. L'accès direct aux métadonnées présente indéniablement des avantages pratiques. De plus, les autorités ont assuré aux rapporteurs, lors des entretiens de Varsovie, que seuls certains agents désignés des forces de police avaient directement accès aux métadonnées chez les fournisseurs de services TIC[110], 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 (le coût a d'ailleurs contribué à limiter le recours à cette méthode dans d'autres pays, mais ne semble pas être un facteur important en Pologne), 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 (comme ils le font dans certains pays, tels le Royaume-Uni ou la Suède), 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 (se reporter aux paragraphes 110 et suivants, qui traitent de l'autorisation et du contrôle de la collecte de métadonnées).

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.

125. En tout état de cause et en conclusion, l'accès direct ne fait que renforcer et justifier davantage encore la nécessité de mettre en place un dispositif efficace de contrôle.

d. Obligation d'archivage

126. La Cour européenne des droits de l'homme a estimé que l'obligation faite aux services pratiquant des interceptions de conserver des archives est particulièrement importante pour que l'organe de contrôle ait effectivement accès au détail des surveillances effectuées[111]. Cela est d'autant plus vrai pour la collecte de métadonnées, du fait que dans sa version actuelle, la loi ne prévoit pas de contrôle juridictionnel préalable de ces opérations. Ces archives devraient présenter, au moins brièvement, les motifs de la surveillance, en s'appuyant sur des faits spécifiques. Les raisons avancées devraient être suffisamment détaillées pour que l'organe de surveillance soit à même de vérifier que l'action de la police était raisonnable.

127. Ces archives devraient par ailleurs toujours être ouvertes à la consultation pour examen indépendant. Le protocole technique d'accès aux métadonnées (en cas d'accès direct) devrait garantir que l'agent concerné ne puisse pas y accéder sans laisser de traces. Les organes de contrôle devraient être habilités à procéder à l'improviste à des vérifications sur place, à obtenir tous les documents nécessaires, ainsi que les témoignages des agents sous serment, etc. Enfin, la loi devrait faire de l'absence d'archives ou de leur inexactitude une grave faute professionnelle, voire une infraction pénale.

[110] Il a été dit aux rapporteurs que sur les quelque 102 000 agents des forces de police, « quelques centaines » seulement sont autorisés à consulter des métadonnées. La police désigne un point de contact unique entre elle et les opérateurs de télécommunication et les fournisseurs d'accès Internet au niveau national, communal et régional.

[111] Affaire *Kennedy*, citée précédemment, paragraphe 165 ; *Roman Zakharov*, citée précédemment, paragraphe 272.

E. Responsabilité juridique des agents de l'Etat

128. Les principes 15, 16 et 17 du rapport des Nations unies sur le contrôle des services de renseignements[112] insistent sur l'importance de la responsabilité pénale, civile et autre des agents de l'Etat participant à des opérations de surveillance en ce qui concerne les infractions au droit interne et le non-respect des obligations internationales relatives aux droits de l'homme. La Commission de Venise souscrit pleinement à ces principes. Les rapporteurs croient comprendre que la responsabilité pénale pour abus de surveillance serait traitée dans d'autres textes de loi (comme le Code pénal). Mais il importe de garantir, si nécessaire par un renvoi dans la loi aux dispositions afférentes d'autres textes, qu'en matière de collecte de métadonnées ou de surveillance secrète, toute ingérence dans la vie privée ou tout détournement de pouvoirs de l'Etat graves et délibérés constitue clairement une infraction pénale.

129. La Commission de Venise recommande d'engager la responsabilité juridique non seulement en cas d'atteinte matérielle à la vie privée d'une personne, mais aussi en cas de non-respect plus « formel » de la procédure (comme le manquement à enregistrer dûment les résultats d'une surveillance ou à détruire les informations dans le délai imparti, ou encore leur communication à des tiers non autorisés), même s'il peut se révéler parfois difficile d'établir le lien entre une infraction de ce type et une ingérence dans vie privée d'une personne.

VII. Conclusions

130. La Commission de Venise se félicite des efforts déployés le législateur polonais pour mettre en œuvre l'arrêt du 30 juillet 2014 du Tribunal constitutionnel de Pologne. Les modifications apportées en 2016 à la loi reprennent bon nombre des recommandations qui figuraient dans l'arrêt ci-dessus mentionné.

131. La Commission de Venise observe que de nombreux pays sont à présent confrontés à de réelles menaces liées au terrorisme et au crime organisé. La CEDH leur laisse une marge d'appréciation quant à l'équilibre à trouver entre sécurité et liberté. Le législateur polonais est loin d'être le seul à s'être attiré de nombreuses critiques sur ce point. Et le gouvernement polonais n'est pas non plus le seul à réagir lentement à l'évolution de l'opinion publique et aux arrêts de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme, selon lesquels la surveillance des métadonnées constitue une ingérence notable dans la vie privée.

132. Ceci étant, les garanties procédurales et les conditions matérielles définies dans la loi sur la police en ce qui concerne la mise en place de mesures de surveillance secrète ne suffisent encore pas à prévenir le recours excessif à cette méthode ni les ingérences indues dans la vie privée des individus.

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) ;

[112] Voir le rapport de l'ONU intitulé *Compilation des bonnes pratiques concernant les cadres juridique et institutionnel et des mesures propres à garantir le respect des droits de l'homme par les services de renseignements dans le cadre de la lutte antiterroriste*, Martin Scheinin, cité précédemment.

- 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.

134. La Commission de Venise reste à la disposition des autorités polonaises pour tout complément d'assistance dont elles pourraient avoir besoin si elles décident de revenir sur la législation analysée dans le présent avis.