



Proposition de loi en vue de l'instauration d'une obligation de notification active pour certaines méthodes spécifiques de collecte de données

Avis de l'Institut fédéral pour la protection et la promotion des droits humains

Avis n° 3/2021 du 4 juin 2021

L'Institut fédéral pour la protection et la promotion des droits humains

L'Institut fédéral pour la protection et la promotion des droits humains (IFDH) a été créé par la loi du 12 mai 2019. L'objectif de l'IFDH est de contribuer à la protection et à la promotion des droits humains en Belgique. Le présent avis s'inscrit dans la mission de conseil du gouvernement fédéral et du Parlement, sur toute question relative aux droits humains, soit à leur demande, à l'instar du présent avis, soit de sa propre initiative.

L'IFDH exerce cette mission dans les limites de son mandat, qui couvre toutes les questions relatives à la protection des droits humains de compétence fédérale et pour lesquelles aucun autre organisme sectoriel n'est compétent. Lors de la préparation de cet avis, un organe sectoriel, le Comité permanent R, a été consulté. Les propos ici-tenus n'engagent que l'IFDH.

1. Introduction

Le 10 mai 2021, l'IFDH a été saisi d'une demande d'avis sur la proposition de loi modifiant la loi organique des services de renseignement et de sécurité du 30 novembre 1998 (ci-après dénommée loi organique), en vue d'introduire une obligation de notification active pour certaines méthodes spécifiques de collecte de données.¹

Dans l'exposé des motifs de la proposition de loi, les auteurs expliquent qu'il n'existe actuellement en Belgique aucune procédure de notification pour l'application des méthodes de renseignement prévues par la loi organique. Cette situation est le résultat de deux annulations par la Cour constitutionnelle des dispositions législatives adoptées en la matière, car elles n'offraient pas de garanties suffisantes au regard des droits humains, notamment parce qu'elles ne consacraient qu'une obligation de notification passive (c'est-à-dire à la demande de la personne concernée) mais pas d'obligation de notification active. La Cour européenne des droits de l'homme a souligné à plusieurs

¹ Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité en vue de l'instauration d'une obligation de notification active pour certaines méthodes spécifiques de collecte de données, *Doc. Parl. Chambre*, 2020-2021, n° 55-1763/001.

reprises la nécessité d'un cadre juridique adéquat et cohérent pour la protection des articles 8 et 13 de la Convention, et l'obligation de notification joue à cet égard un rôle important.² La Cour constitutionnelle a, pour sa part, jugé qu'une simple obligation de notification passive est insuffisante pour garantir le droit à un recours effectif et le droit au respect de la vie privée. Une obligation de notification active est donc nécessaire.

Selon les auteurs de la proposition de loi, l'objectif est d'introduire une nouvelle procédure de notification qui comporte les garanties nécessaires, tant en ce qui concerne l'obligation de notification active que passive.

2. Cadre en matière de droits humains

a. Droits humains concernés

La surveillance est un enjeu complexe pour les droits humains. Son caractère secret est à la fois nécessaire pour **sauvegarder certains intérêts fondamentaux de l'Etat** et un réel risque pour les droits des individus visés,³ en particulier le **droit à la vie privée et familiale** et le **droit à un recours effectif**. Les services de renseignement et de sécurité doivent donc veiller au respect de ces droits, conformément à l'encadrement de ces méthodes prévu par le législateur.

Le **droit au respect de la vie privée et familiale** protège les personnes contre les ingérences dans leur vie intime, leur famille, leur domicile ou leur correspondance.⁴ Or, comme le rappelle le Sénat à la veille de l'adoption de l'**article 22 de la Constitution**, se multiplient aujourd'hui « *des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des techniques de l'information, les mesures d'investigation, d'enquête et de contrôle menées par les pouvoirs publics et organismes privés, dans l'accomplissement de leurs fonctions ou de leurs activités* ». ⁵ Le fait que des mesures de surveillance se déroulent **à l'insu de la personne concernée** augmente la gravité de l'ingérence.⁶

² Voir e.a. Cour E.D.H. (grande chambre), *Big Brother Watch e.a. c. Royaume-Uni*, arrêt du 25 mai 2021, n° 58170/13, 62322/14 et 24960/15, §§ 337 et 357; Cour E.D.H. (grande chambre), *Centrum för Rättvisa c. Suède*, arrêt du 25 mai 2021, n° 35252/08, §§ 251 et 271; Cour E.D.H. (grande chambre), *Roman Zakharov c. Russie*, arrêt du 4 décembre 2015, n° 47143/06, § 234.

³ Voir e.a. Cour E.D.H. (grande chambre), *Big Brother Watch e.a. c. Royaume-Uni*, arrêt du 25 mai 2021, n° 58170/13, 62322/14 et 24960/15, § 336: « *Le contrôle et la supervision des mesures de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé. En ce qui concerne les deux premières phases, la Cour note 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. Puisque la personne concernée sera donc nécessairement dans l'impossibilité d'introduire de son propre chef un recours effectif ou de prendre une part directe à quelque procédure de contrôle que ce soit, il est indispensable que les mécanismes existants procurent en eux-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le contrôle juridictionnel offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière* ». Voir également Cour E.D.H. (grande chambre), *Centrum för Rättvisa c. Suède*, arrêt du 25 mai 2021, n° 35252/08, § 250.

⁴ Art. 22 de la Constitution ; art. 8 de la Convention européenne des droits de l'homme.

⁵ *Doc. Parl.*, Sénat, S.E., 1991-1992, n°100-4/2, p.3, cité dans C. cons., arrêt n°41/2019 du 14 mars 2019, B.8.3.

⁶ C. cons., arrêt n°41/2019, *op cit.*, B.14.

Assurer le **droit à un recours effectif** en matière de surveillance est un enjeu tout aussi crucial pour les droits humains⁷. Il est la clé de voûte du système de protection des droits humains en Europe.⁸ Or, le caractère secret inhérent à ces méthodes de surveillance **rend pratiquement impossible l'exercice d'un recours** pendant l'exécution des mesures. La protection de ce droit impose au législateur de prévoir **des mécanismes d'examen et de contrôle des méthodes de surveillance** : un mécanisme de contrôle secret, indépendant et objectif **avant et pendant la période d'exécution des mesures**, incarné en Belgique par la Commission BIM, et **l'ouverture de voies de recours une fois les méthodes connues de l'individu**.⁹ Dans son examen de la législation belge alors applicable, la **Cour constitutionnelle** rappelle l'importance du contrôle de la surveillance lorsque celle-ci a cessé :

« [...] la question de la notification a posteriori de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (*Klass et autres*, précité, § 57, et *Weber et Saravia*, décision précitée, § 135) ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, (...) (*Kennedy*, précité, § 167) ».¹⁰

Ce raisonnement est partagé par la **Cour de Justice de l'Union européenne**, selon laquelle le contrôle des mesures de surveillance ne peut se concevoir sans accorder la possibilité d'un examen juridictionnel effectif au justiciable concerné. Dans l'arrêt **ZZ. c. Secretary of State**, la Cour déclare que « les États membres sont tenus de prévoir, d'une part, un contrôle juridictionnel effectif tant de l'existence et du bien-fondé des raisons invoquées par l'autorité nationale au regard de la sûreté de l'État que de la légalité de la décision prise en application de l'article 27 de la directive 2004/38 ainsi que, d'autre part, des techniques et des règles relatives à ce contrôle (...) ».¹¹

Le respect de la vie privée et du droit au recours effectif est un **prérequis à toute forme de collecte d'informations** par les services de renseignement. Si la protection des intérêts fondamentaux de l'État peut justifier une **spécialisation du contrôle vers une juridiction habilitée**, et un report de la phase d'information de l'individu visé, les méthodes exceptionnelles de surveillance ne peuvent se faire ni dans le secret complet ni sans contrôle, aussi bien avant et pendant la surveillance que lorsqu'elle a pris fin.

b. Garanties prévues par le législateur

Le législateur est bien conscient des ingérences aux droits humains engendrées par certaines mesures sollicitées par les services de renseignement et de sécurité. Par conséquent, il a veillé à **introduire des garanties** dans la législation applicable à ces services afin d'éviter les abus et d'y permettre un certain **contrôle, y compris juridictionnel**¹². La loi organique du 30 novembre 1998 introduit trois catégories

⁷ Art. 13 de la Convention européenne des droits de l'homme ; art. 47 de la Charte des droits fondamentaux de l'Union européenne.

⁸ Cour E.D.H. (grande chambre), *Kudla c. Pologne*, arrêt du 26 octobre 2000, requête n° 30210/96, § 155.

⁹ Voir à ce sujet les arrêts de la Cour E.D.H. *Klass et autres c. Allemagne*, 6 septembre 1978, n° 5920/71, §§ 68 et 69 et *Rotaru c. Roumanie* (grande chambre), 4 mai 2000, n° 28341/95, § 69. En matière de surveillance, voir également *Kennedy c. Royaume-Uni*, 18 mai 2010, n°26839/05, et *Roman Zakharov c. Russie* (grande chambre), 4 décembre 2015, n° 47143/06.

¹⁰ Cour E.D.H. (grande chambre), *Roman Zakharov c. Russie*, *op. cit.*, § 234, cité dans C. cons, arrêt n° 41/2019, B.10.

¹¹ C.J.U.E., *ZZ. c. Secretary of State*, arrêt du 4 juin 2013, C-300/11, §§ 57-58, disponible sur www.curia.eu.

¹² La Commission BIM est en effet composée par trois magistrats et présidée par un juge d'instruction.

de méthodes de collecte de données par les services de sécurité et de renseignement : **les méthodes ordinaires, spécifiques et exceptionnelles**. Ces trois catégories sont caractérisées par leur **degré croissant d'intrusion dans la vie privée des individus concernés, et par leur subsidiarité décroissante** : les méthodes spécifiques ne peuvent être utilisées que si les méthodes ordinaires se révèlent insuffisantes pour permettre l'aboutissement de la mission de renseignement¹³, et les méthodes exceptionnelles que si les méthodes spécifiques, à leur tour, ne permettent pas la récolte des informations recherchées.¹⁴ Des conditions supplémentaires sont également requises pour l'autorisation de méthodes exceptionnelles. Elles exigent un **certain degré de gravité représenté par la menace potentielle pour la sécurité nationale**,¹⁵ nécessitent **l'autorisation préalable écrite du dirigeant du service de sécurité** concerné et **l'avis conforme de la Commission BIM**. Elles sont également limitées à une **durée maximale de deux mois**, éventuellement renouvelables

Le rapport 2019 du Comité permanent R contient de nombreuses informations relatives à l'utilisation des méthodes spécifiques et exceptionnelles.¹⁶ La Sûreté de l'Etat a, cette même année, obtenu 1781 autorisations d'avoir recours à des méthodes spécifiques et 449 autorisations d'avoir recours à des méthodes exceptionnelles. Cette utilisation est en nette hausse : au sein de la Sûreté de l'Etat, l'utilisation de méthodes spécifiques a augmenté de moitié en cinq ans¹⁷, et **le recours aux méthodes exceptionnelles a plus que triplé** sur la même période.¹⁸ Les méthodes exceptionnelles privilégiées sont **les écoutes téléphoniques**¹⁹, **la collecte d'informations bancaires**²⁰ et **l'introduction au sein d'un système informatique**²¹. Ces mesures visent principalement **le terrorisme** (en ce compris la surveillance des processus de radicalisation) et **l'espionnage**.²² Le rapport 2019 du Comité permanent R ne semble pas contenir de chiffres relatifs aux demandes de notification adressées par des justiciables aux services de sécurité compétents. Or, la loi organique prévoit explicitement un rapport annuel du Comité R sur les demandes adressées aux services de renseignement. En outre, le rapport 2019 indique que **le Comité permanent R n'a eu aucune saisine d'un individu entre 2013 et 2019, à l'exception d'une plainte en 2016**. Il n'a également reçu aucune demande de la part de la Commission Vie Privée, devenue l'Autorité de Protection des données, sur la même période.²³ Il semblerait donc

¹³ Art. 18/3, §1er, alinéa 1er, loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *M.B.*, 18 décembre 1998.

¹⁴ Art. 18/9, §2, loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *op. cit.*

¹⁵ Art. 18/9, §3, loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *op. cit.*

¹⁶ Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport d'activités 2019, Intersentia, Bruxelles, 2020, p. 44 et suiv.

¹⁷ 1143 méthodes spécifiques en 2015 pour 1781 en 2019. Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport d'activités 2019, *op. cit.*, p. 40.

¹⁸ 128 méthodes exceptionnelles en 2015 pour 449 en 2019.

¹⁹ Art. 18/7, loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *op. cit.* 255 autorisations ont été accordées en 2019.

²⁰ Art. 18/5, loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *op. cit.* 95 autorisations ont été accordées en 2019.

²¹ Art. 18/6, loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *op. cit.* 48 autorisations ont été accordées en 2019.

²² Qui justifient respectivement 1118 et 777 autorisations pour des méthodes spécifiques et exceptionnelles. Les chiffres ne sont pas ventilés selon la méthode utilisée, contrairement aux catégories précédentes.

²³ Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport d'activités 2019, *op. cit.*, p. 52. Il est vraisemblable que cette absence de demande de notification peut s'expliquer en partie par l'annulation des dispositions ordonnant l'obligation de notification passive par la Cour constitutionnelle en 2011 et en 2019. Toutefois, une telle explication résulterait d'une mauvaise compréhension des annulations de l'article 2 § 3 de la loi organique du 30 novembre 1998 : la Cour n'y interdit pas l'obligation de notification passive. Au contraire, elle estime que celle-ci ne garantit pas suffisamment les droits à la vie privée et à un recours effectif et qu'il revient au législateur de consacrer également une obligation de notification active.

qu'aucune demande de notification passive n'ait été portée à la connaissance du Comité permanent R au cours de cette période.²⁴

A l'heure actuelle, il n'existe pas d'obligation de notification active d'une personne qui aurait fait l'objet de mesures exceptionnelles de surveillance, et l'existence d'une obligation de notification sur demande de l'intéressé est débattable. Par conséquent, le législateur a tenté à plusieurs reprises de renforcer les garanties des droits humains des justiciables, notamment lors de l'adoption des **lois du 4 février 2010 et du 30 mars 2017** (*infra*).

c. *L'obligation de notification passive de la loi du 4 février 2010 : un cadre insuffisant pour la protection de la vie privée et du recours effectif*

La proposition de loi examinée succède à deux lois relatives au recueil de données par les services de renseignement et de sécurité. Ces normes ont **toutes deux été partiellement annulées par la Cour constitutionnelle** en raison de sérieuses critiques sur les garanties pour les droits humains.

La **loi du 4 février 2010** relative aux méthodes de recueil des données par les services de renseignement et de sécurité²⁵, introduisait dans la loi organique une **obligation de notification passive**. Sous certaines conditions, la personne qui en faisait la demande auprès du service concerné était informée de l'utilisation antérieure de certaines méthodes exceptionnelles à son encontre. La loi précisait que la notification n'intervenait qu'**après un délai de cinq ans** à partir de la fin de la méthode, et pour autant qu'aucune nouvelle donnée n'ait été recueillie au sujet du demandeur au cours de ce délai. Cette double condition limitait fortement la possibilité de connaître de l'existence d'une méthode de surveillance.

Saisie d'un recours en annulation, la Cour constitutionnelle note en 2011 que **la notification a posteriori de l'existence de mesures de surveillance est indispensable pour reconnaître un recours effectif** : la notification est « *indissociablement liée au caractère effectif des recours juridictionnels, et donc à l'existence de garanties effectives contre les abus.*²⁶ Le raisonnement de la Cour précise : « *S'il n'est pas avisé des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice.* »²⁷.

La Cour rappelle que le législateur était animé du souci de **trouver un équilibre entre la protection des intérêts fondamentaux de l'État et le respect des droits humains individuels**. Elle souligne que l'introduction d'une obligation de notification vise à **améliorer le contrôle des services de renseignement** et le respect des droits des individus concernés par ces mesures de surveillance. Cette réflexion la conduit à avaliser l'**exclusion des méthodes ordinaires du champ d'application** de l'obligation de notification, considérant que cette exclusion est raisonnable puisque les méthodes spécifiques et exceptionnelles portent davantage atteinte aux droits humains. Ce même souci d'un équilibre entre intérêts de l'État et de l'individu justifie également qu'**un certain délai** puisse s'écouler entre la fin de la mesure et la notification prévue.²⁸ La Cour ne précise pas si un délai de cinq ans lui

Interpréter cet arrêt pour justifier un refus d'une demande de notification conforme aux conditions stipulées par le législateur serait contraire au raisonnement de la Cour.

²⁴ L'IFDH a interrogé le Comité permanent R pour confirmer cette hypothèse mais celui-ci n'a pas pu y répondre endéans les délais impartis au dépôt de cet avis.

²⁵ Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, *M. B.*, 10 mars 2010.

²⁶ C. cons., arrêt n°145/2011, *op. cit.*, B.86.

²⁷ *Ibidem*. Nous soulignons.

²⁸ C. cons., arrêt n°145/2011, *op. cit.*, B.87.

paraît suffisant, mais il demeure soumis à un examen de proportionnalité et ne peut dépasser ce qui est strictement nécessaire.

La Cour estime donc que la loi ne garantit pas assez le respect du droit à la vie privée, à l'égalité et à la non-discrimination et **annule le dispositif ne consacrant qu'une obligation de notification passive**. Elle annule également l'interdiction faite aux personnes morales d'introduire une demande de notification.²⁹

d. *L'obligation de notification passive de la loi du 30 mars 2017*

Le législateur entend répondre aux objections de la Cour constitutionnelle en adoptant **la loi du 30 mars 2017**.³⁰ Il consacre à nouveau une obligation de notification passive dans des termes similaires à ceux de la loi du 4 février 2010 : la notification se fait **après une demande de l'intéressé** justifiant d'un intérêt personnel et légitime. Les conditions pour demander cette notification sont généralement plus strictes qu'en 2010, et **l'équilibre entre intérêts de l'État et ceux de l'individu penche plus nettement en faveur des autorités publiques**. La demande n'est recevable que dix ans après la fin de la méthode, au lieu de cinq ; elle ne concerne plus que trois méthodes exceptionnelles de renseignement sur sept ; elle ne peut explicitement ni nuire aux relations avec des États étrangers ni avec des organisations internationales, ni conduire à divulguer l'identité de tiers informateurs.

Saisie d'un **nouveau recours en annulation**, la Cour constitutionnelle se prononce dans un arrêt du 14 mars 2019. La Cour constitutionnelle rappelle que la notification de la méthode de surveillance a **pour principal objet de permettre**, le cas échéant, **à une personne de contester la légalité de la mesure dont elle a fait l'objet**. Or, en l'absence d'une obligation de notification active, la possibilité de pouvoir introduire un tel recours est « *uniquement théorique* ». ³¹ Une certaine forme de levée du secret est donc indispensable pour permettre l'accès à un recours effectif, et celle-ci ne peut être laissée à la seule initiative d'un justiciable non informé. La Cour en conclut qu'**en omettant de consacrer une forme de notification active de la méthode de surveillance, le législateur n'a pas** garanti les droits à la vie privée et à un recours effectif, et **annule l'obligation de notification passive** contenue dans la loi du 30 mars 2017.

Ces constats ont conduit plusieurs acteurs à **critiquer les garanties des droits humains** intégrées aux règles encadrant les méthodes spécifiques et exceptionnelles de surveillance. Dans son rapport sur la Belgique, la **Rapporteuse spéciale des Nations-Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste**, Fionnuala Ní Aoláin, rappelle que **la protection de la vie privée favorise l'exercice d'un grand nombre de droits humains**.³² Elle constate que les services belges de renseignement peuvent collecter des informations personnelles sur des individus **sans que ceux-ci soient soupçonnés d'avoir commis une infraction pénale**.³³ Elle poursuit :

«[s]i le fait d'être inscrit dans la base de données [conjointe des combattants terroristes] ne constitue pas une mesure pénale, il a généralement de lourdes conséquences sur les droits de

²⁹ C. cons., arrêt n°145/2011, *op. cit.*, B.92.

³⁰ Loi du 30 mars 2017 modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et l'article 259bis du Code pénal, *M.B.*, 28 avril 2017.

³¹ C. cons., arrêt n°41/2019, *op. cit.*, B. 15.2.

³² Conseil des droits de l'homme, rapport de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, visite en Belgique, 8 mai 2019, U.N. doc. A/HRC/40/52/Add.5, § 52.

³³ Conseil des droits de l'homme, rapport de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, § 56.

*l'homme des personnes concernées, notamment des restrictions de liberté qui peuvent constituer des atteintes aux droits énoncés à l'article 5 de la Convention européenne des droits de l'homme. La Rapporteuse spéciale est d'autant plus préoccupée que les possibilités de retirer une personne et les renseignements qui la concernent de la base de données sont très limitées. (...) Les possibles incidences néfastes sur les personnes inscrites dans la base de données lorsqu'elles étaient mineures sont particulièrement inquiétantes ».*³⁴

La Rapporteuse spéciale estime ensuite qu'**il manque un véritable mécanisme judiciaire indépendant complémentaire au contrôle de la collecte et du traitement des données** par le Comité permanent R, l'Organe de contrôle de l'information policière et l'Autorité de protection des données. Vie privée et droit à un recours effectif sont indissociables et essentiels à l'encadrement des mesures de surveillance secrètes.³⁵

e. *Conséquences sur d'autres droits que la vie privée*

L'enjeu – et les conséquences – de faire l'objet d'un dossier au sein des services de renseignement **dépasse le respect du droit à la vie privée des individus concernés**. Une collecte abusive de données pose également des risques, au moins indirects, pour la liberté d'expression, la liberté d'association, la liberté religieuse et le droit à un procès équitable.³⁶ Comme le rappelle la Rapporteuse spéciale des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste : « *les atteintes à la vie privée peuvent avoir des incidences négatives croisées, non seulement sur les droits civils et politiques mais aussi sur les droits économiques, sociaux et culturels.* »³⁷

Les fichiers rassemblés par les services de renseignement et de sécurité sont notamment utilisés pour appuyer la décision des autorités publiques dans un certain nombre de situations :

- Des interdictions de travailler dans certains secteurs sensibles (aéroports, centrales nucléaires, Défense, certaines institutions européennes, etc.), lorsque ceux-ci demandent de disposer d'une attestation ou d'un avis de sécurité positif³⁸ ;
- Des refus d'octroi de la nationalité belge en cas de « faits personnels graves »³⁹ ;
- La fermeture d'établissements par les autorités communales sur la base d'une suspicion d'activité terroriste⁴⁰ ;

³⁴ *Ibidem*.

³⁵ Conseil des droits de l'homme, rapport de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, §60.

³⁶ Voir, par exemple, Commissaire aux droits de l'homme du Conseil de l'Europe, [Democratic and effective oversight of national security services](#), Issue paper, Strasbourg: Conseil de l'Europe, mai 2015; Voir également Haut-Commissariat des Nations unies aux droits de l'homme, [Le droit à la vie privée à l'ère du numérique](#), UN Doc. A/HRC/39/29, 3 août 2018.

³⁷ Conseil des droits de l'homme, rapport de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *op. cit.*, § 52.

³⁸ Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.*, 7 mai 1999.

³⁹ Notion visée aux articles 1er §2 4° et 15 §3 du Code de la nationalité belge du 28 juin 1984, *M.B.*, 12 juillet 1984.

⁴⁰ Art. 134septies, nouvelle loi communale du 24 juin 1998 (version de la Région de Bruxelles-Capitale), *M.B.*, 3 septembre 1998: « *lorsqu'il existe des indices sérieux selon lesquels se déroulent dans un établissement des faits constitutifs d'une des infractions terroristes visées au livre II, titre Ier ter, du Code pénal, le bourgmestre peut,*

- Des refus de délivrance de passeport ou de titre de voyage belge vers certaines destinations spécifiques (Turquie, Irak, etc.) lorsque les autorités estiment que la personne est à risque de devenir un combattant terroriste⁴¹ ;
- La révocation du titre de séjour et l'expulsion des étrangers du territoire belge si ceux-ci représentent un trouble « grave » d'ordre public ou de sécurité nationale⁴²;
- Une surveillance par la Cellule de sécurité intégrale locale.⁴³

Ces mesures peuvent être nécessaires pour **garantir la sécurité nationale et l'ordre public**. Toutefois, leurs conséquences sur les droits individuels n'en sont pas moins considérables et il importe qu'existe **un contrôle des éventuels abus**. L'envoi « actif » d'une notification par les autorités conformément aux conditions énoncées dans la proposition de loi examinée peut permettre à ces personnes de **prévenir certaines de ces restrictions de leurs droits humains**. Une personne qui serait informée qu'elle a fait l'objet d'une méthode exceptionnelle de recherche pourrait ainsi introduire un recours destiné à faire examiner par une juridiction indépendante le sérieux du dossier sur lequel ces mesures se fondent ou pourraient se fonder, avant d'avoir souffert des conséquences négatives associées à l'existence de son dossier. En cas de collecte d'informations qui se sont avérées non fondées par rapport à la mission de renseignement, la personne pourrait demander la correction des informations. En cas d'usage abusif de méthodes de surveillance, elle pourrait obtenir en outre une indemnité.

3. Recommandations de l'IFDH

a. *Appréciation générale de la proposition de loi*

Les arrêts de la Cour constitutionnelle, appuyés par la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de Justice de l'Union européenne, requièrent que les individus **soient informés des méthodes de surveillance dont ils ont fait l'objet** de la part des services de renseignement et de sécurité, **particulièrement lorsqu'il s'agit de méthodes exceptionnelles** impliquant une profonde violation de la vie privée. Le législateur doit veiller à consacrer un équilibre entre intérêts de l'État et droits humains des particuliers. Ses précédentes tentatives de trouver cet équilibre ont échoué et **seule une forme d'obligation active** peut garantir le respect des droits procéduraux des individus.

L'IFDH se réjouit que l'objet de la proposition de loi soit précisément la consécration d'une obligation de notification active. Il note que les conditions d'exercice de ce droit sont **moins strictes que celles prévues par la loi du 30 mars 2017** annulée par la Cour constitutionnelle : le délai de notification intervient cinq ans après la fin de la mise en œuvre de la méthode ; une procédure d'examen des refus de notification par la Commission BIM est détaillée ; et il ne suffit plus qu'un nouvel élément soit ajouté au dossier pour justifier automatiquement un refus de notification. Ce

après concertation préalable avec les autorités judiciaires, et après avoir entendu le responsable dans ses moyens de défense, décider de fermer cet établissement pour une durée qu'il détermine».

⁴¹ Art. 5, loi du 10 août 2015 portant modification du Code consulaire, *M.B.*, 24 août 2015.

⁴² Loi du 24 février 2017 modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers afin de renforcer la protection de l'ordre public et de la sécurité nationale, *M.B.*, 29 avril 2017 ; Loi du 15 mars 2017 modifiant l'article 39/79 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, *M.B.*, 29 avril 2017.

Ces lois sont également citées dans le rapport 2019 sur la Belgique de la Rapporteuse spéciale des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme, *op. cit.*, § 68.

⁴³ Loi du 30 juillet 2018 portant création des cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, *M.B.*, 14 septembre 2018.

dernier élément était particulièrement important puisqu'il risquait de rendre l'obligation de notification active purement théorique. L'existence d'un rapport annuel du Comité permanent R à la Chambre des représentants renforce également le dispositif et assure une certaine transparence à son application.

L'IFDH estime toutefois que certaines précisions peuvent être apportées à la proposition de loi afin de renforcer la protection des droits humains prévue dans celle-ci.

Dans ce contexte, il peut d'abord être souligné que la proposition de loi s'intitule « proposition de loi modifiant la loi du 30 novembre 1998 (...) en vue de l'instauration d'une obligation de notification active pour certaines méthodes **spécifiques** de collecte de données » (nous soulignons). Toutefois, comme indiqué ci-dessus, la loi distingue trois types de méthodes de renseignement : ordinaires, spécifiques et exceptionnelles, classées en fonction de leur degré d'ingérence dans la vie privée. La proposition de loi actuelle ne porte toutefois que sur les méthodes exceptionnelles. Le titre est donc quelque peu trompeur et pourrait être modifié.

En outre, l'IFDH souhaite formuler huit recommandations. Ces huit **recommandations** permettraient de clarifier l'application de l'obligation de notification active et de rendre plus effectifs la protection de la vie privée et le droit au recours dans le contexte de méthodes de surveillance.

b. *Champ d'application*

i. **Absence de certaines méthodes exceptionnelles**

La proposition de loi (art. 2) concerne les méthodes exceptionnelles visées aux articles 18/12 de la loi organique (fouille de lieux privés non accessibles au public et du contenu d'objets fermés à clé qui s'y trouvent), 18/14 (ouverture du courrier confié à un opérateur postal et examen de son contenu) et 18/17 (interception de communications, examen et enregistrement de celles-ci), mais pas les méthodes exceptionnelles visées aux articles 18/11, 18/13, 18/15 et 18/16. L'IFDH n'aperçoit pas clairement sur quelle base se fonde cette distinction apparente entre méthodes exceptionnelles. L'exposé des motifs n'aborde pas non plus cette question.

Les méthodes exceptionnelles qui ne font pas l'objet de la modification législative proposée impliquent pourtant des intrusions significatives dans la vie privée. Elles incluent entre autres la possibilité de :

- pénétrer dans des lieux qui ne sont pas accessibles au public et les observer par des moyens techniques (art. 18/11 de la loi organique) ;
- requérir les données bancaires (art. 18/15 de la loi organique) ;
- et d'accéder aux systèmes informatiques et acquérir leurs données (art. 18/16 de la loi organique).

L'IFDH considère qu'une obligation de notification devrait en principe également s'appliquer à ces méthodes.

Le recours à des personnes morales pour collecter des données peut également avoir un impact potentiellement important sur la vie et les activités des individus (art. 18/13). La proposition de loi n'explique pas non plus pourquoi cette méthode serait *a priori* incompatible avec une obligation de notification active.

Recommandation n° 1

Le fait que l'utilisation des méthodes exceptionnelles mentionnées dans les articles 18/11, 18/13, 18/15 et 18/16 de la loi organique n'entraîne pas d'obligation de notification active doit être justifié. En l'absence d'une telle justification, ces méthodes exceptionnelles devraient également entrer dans le champ d'application de la loi.

c. Modalités pratiques

i. **Seul un préjudice grave et raisonnablement prévisible pour une enquête de renseignement peut justifier une exception.**

L'article 2 de la proposition de modification de la loi introduit une obligation de notification active au plus tard cinq ans après la fin de la méthode en question, mais avec trois exceptions possibles, à savoir lorsque la notification pourrait (1) nuire à l'enquête de renseignement, (2) être incompatible avec la protection des sources, ou (3) nuire aux relations de la Belgique avec d'autres pays ou institutions supranationales.

En ce qui concerne la première exception, à savoir l'hypothèse qu'une notification pourrait nuire à une enquête de renseignement, l'IFDH est d'avis qu'une condition plus stricte devrait être prévue, car la simple possibilité qu'une notification puisse causer un préjudice pourrait conduire dans la pratique à une situation où cette exception est invoquée trop rapidement et trop fréquemment, même lorsque cela n'est pas strictement nécessaire.

L'IFDH considère que, pour cette première exception, seuls les dommages **graves** et les dommages **raisonnablement prévisibles** doivent être retenus comme exceptions à l'obligation de notification active.

Recommandation n° 2

Dans l'article 2 proposé, qui remplace l'article 2, §3 de la loi organique, la première condition de l'obligation de notification active devrait être reformulée comme suit : "1° la notification ne causera pas de préjudice grave et raisonnablement prévisible à ladite enquête".

ii. **Seul un préjudice grave et raisonnablement prévisible aux relations internationales peut justifier une exception.**

En ce qui concerne la troisième exception, c'est-à-dire lorsque la notification « peut nuire aux relations de la Belgique avec d'autres pays ou institutions supranationales », l'IFDH est également d'avis que cette condition doit être encadrée plus strictement. A nouveau, il craint que cette exception soit définie trop approximativement et qu'elle soit interprétée trop largement.

L'IFDH suggère donc que cette condition soit renforcée pour que l'exception ne concerne plus que les dommages **graves**, et les dommages **raisonnablement prévisibles** et non, comme la proposition de loi actuelle l'indique, tous les dommages possibles. Ces deux éléments sont par ailleurs également consacrés par la législation néerlandaise, qui est citée par les auteurs de la proposition.⁴⁴

⁴⁴ L'article 59.7.b de la loi néerlandaise sur les services de renseignement et de sécurité stipule que: "L'obligation d'enquête, telle que visée au paragraphe 1er, s'éteint si l'on peut raisonnablement s'attendre à ce que la présentation d'un rapport concernant l'exercice du pouvoir spécial en question ait pour résultat : b. que les relations avec d'autres pays et avec des organisations internationales soient gravement compromises". Traduit

Recommandation n° 3

Dans l'article 2 proposé, qui remplace l'article 2, §3 de la loi organique, la troisième condition de l'obligation de notification active devrait être reformulée comme suit : "3° la notification ne cause pas de préjudice grave et raisonnablement prévisible aux relations que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales."

iii. Un contrôle strict des exceptions prévues

L'IFDH est préoccupé par la possibilité que les exceptions prévues par la proposition de loi soient **interprétées de manière trop large**. Cela conduirait à une situation où il serait trop facilement décidé qu'une notification comporte un risque (indirect) de dommage, ce qui, dans de nombreux cas, rendrait l'obligation de notification purement théorique.

Le principe général devrait être celui de la notification active, avec une interprétation stricte des exceptions.

Il est essentiel que la Commission BIM et le Comité permanent R exercent un contrôle strict. À cette fin, des critères clairs d'application doivent être convenus tant par les services de renseignement et de sécurité que par la Commission BIM et le Comité permanent R.

Recommandation 4

Les exceptions à l'obligation de notification active prévues doivent être interprétées de manière stricte, et un contrôle rigoureux de l'application des exceptions par la Commission BIM et le Comité permanent R est nécessaire. Des critères supplémentaires d'application devraient être élaborés à cette fin.

iv. Une notification dès que possible

En outre, la question se pose des conséquences du cumul des règles proposées. L'application de ces règles implique que même lorsqu'il est établi plus rapidement qu'un préjudice n'est pas (ou plus) prévisible (par exemple, s'il est déjà clair après un an qu'aucun dommage ne serait causé à une enquête de renseignement si la méthode était notifiée), il demeure obligatoire d'attendre jusqu'à cinq ans avant de procéder à la notification. En d'autres termes, il est possible que, même si la notification puisse être faite avant l'expiration du délai sans porter atteinte aux intérêts protégés par l'exception, elle ne soit quand même réalisée qu'après cinq ans.

L'obligation de notification constitue une garantie importante contre l'utilisation abusive des méthodes exceptionnelles. Par conséquent, les personnes qui ont fait l'objet de ces méthodes doivent être notifiées **dès que possible**, c'est-à-dire dès que les conditions imposées sont remplies.

Le **délai** pour un premier examen de la possibilité de notification devrait donc être **réduit à un maximum après la fin de la méthode utilisée**. Par la suite, le refus de notifier devrait être réexaminé chaque année, comme le prévoit la proposition de loi (article 2 *in fine*).

de : "De verplichting tot onderzoek, bedoeld in het eerste lid, vervalt, indien het uitbrengen van een verslag omtrent de uitoefening van de desbetreffende bijzondere bevoegdheid naar redelijke verwachting ertoe leidt, dat: b. betrekking met andere landen en met internationale organisaties ernstig worden geschaad."

Recommandation n° 5

La personne qui a fait l'objet d'une méthode exceptionnelle de collecte de données doit en être informée le plus tôt possible. La notification doit avoir lieu dès qu'il est clair qu'aucune des exceptions ne s'applique, et un premier examen de la possibilité de notifier doit avoir lieu au plus tard un an après la fin de la méthode utilisée.

v. Contrôle de l'impossibilité de notification

Dans la pratique, il ne sera pas toujours possible de joindre la personne qui a fait l'objet d'une méthode exceptionnelle. Toutefois, le chef de service doit faire tous les efforts raisonnables pour informer une personne de la méthode exceptionnelle dont elle a fait l'objet.

Il est important à cet égard que, lorsqu'il reste raisonnablement infaisable de procéder à la notification requise, cela soit **signalé** à la Commission BIM et au Comité permanent R, en exposant les raisons de l'impossibilité de procéder à la notification et les efforts qui ont néanmoins été entrepris.

Recommandation n° 6

Lorsque la personne qui a fait l'objet d'une méthode exceptionnelle ne peut être jointe, l'impossibilité de notification doit être signalée à la Commission BIM et au Comité permanent R, en exposant les circonstances qui ont rendu la notification impossible. Cela permettra de vérifier que tous les efforts raisonnables ont été entrepris pour effectuer la notification.

vi. Informations supplémentaires dans la notification

La proposition de loi (art. 2) stipule que, lors de la notification, le chef de service doit toujours indiquer quelle méthode a été utilisée, pour quelle période et sur quelle base juridique. L'IFDH propose que soit indiqué exactement **quel lieu non accessible au public a fait l'objet de la méthode de récolte de données**.

En outre, chaque notification devrait également mentionner explicitement **les voies de recours** auxquelles la personne ayant fait l'objet de la méthode exceptionnelle peut faire appel,⁴⁵ qu'il s'agisse aussi bien d'une plainte introduite auprès du Comité permanent R⁴⁶ ou d'un contrôle juridictionnel à proprement parler.

Recommandation n° 7

La notification doit également indiquer exactement quel lieu non accessible au public a fait l'objet de la méthode de récolte de données et, en tout état de cause, doit mentionner

⁴⁵ Voir également la recommandation faite par Amnesty International Pays-Bas à la suite de la loi néerlandaise : Amnesty International Nederland, Wetsvoorstel van Wet op de inlichtingen- en veiligheidsdiensten 20xx, 2016, https://www.amnesty.nl/content/uploads/2016/12/wetsvoorstel_wiv_20xx_-_bezwaren_amnesty_nederland.pdf?x22401 (consulté le 25 mai 2021).

⁴⁶ Le droit d'introduire une plainte au sein du Comité permanent R est prévu par l'article 51/3 de la loi organique du 8 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (*M.B.*, 26 juillet 1991).

explicitement les voies de recours dont dispose la personne qui a fait l'objet de cette méthode exceptionnelle.

d. *Possibilités de recours*

L'IFDH est d'avis que le droit à un recours effectif pourrait être mieux protégé dans la proposition de loi. Le droit de recours bénéficierait d'une part de précisions relatives à la nature du recours et d'un mécanisme spécifique destiné à permettre au justiciable concerné d'obtenir la suppression ou la contestation des données illégalement récoltées ou infondées. Ce recours pourrait également conduire à l'indemnisation du préjudice associé à l'utilisation abusive de méthodes de surveillance. Une telle indemnisation serait de préférence établie forfaitairement par le législateur, afin de renforcer la sécurité juridique et d'éviter les sanctions purement symboliques.

Quelle que soit la forme du recours privilégiée par le législateur et la juridiction désignée compétente, il paraît important que les juges disposent du droit d'examiner le dossier, y compris les portions classifiées, et quel le principe du contradictoire y ait cours, quand bien même l'accès à certaines pièces pourrait être refusé au plaignant si leur communication mettrait en péril les intérêts de l'Etat. Le résultat de cette procédure devrait permettre soit la suppression des données renseignées sur le justiciable, soit l'apposition de la décision de justice au dossier, interdisant l'utilisation des données récoltées précédemment. Enfin, il est important que les décisions adoptées à ce sujet soient rendues publiques, avec l'anonymisation des données personnelles du requérant à sa demande. En effet, la visibilité du contrôle des méthodes de surveillance est indispensable à la confiance du public dans les services de renseignement et de sécurité et dans le travail de la justice.

Recommandation n° 8

Il faut inscrire dans la loi un recours *a posteriori* permettant de contester la légalité et la proportionnalité des mesures exceptionnelles de surveillance adoptées. Ce recours pourrait être de nature indemnitaire et forfaitaire, et devrait soit permettre l'effacement des données détenues par les services de renseignement et de sécurité soit permettre le dépôt de la décision de justice au dossier. Les décisions doivent par principe être rendues publiques.

4. Conclusion et recommandations

L'IFDH constate que la proposition de loi instaurant **une obligation de notification active renforce fortement le droit à la vie privée et le droit à un recours effectif** en matière d'utilisation de méthodes exceptionnelles de surveillance par les services de renseignement et de sécurité. La proposition répond assez largement aux critiques émises par la Cour constitutionnelle dans ses arrêts n° 145/2011 et 41/2019 et est, selon l'IFDH, conforme à la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de Justice de l'Union européenne.

L'IFDH n'en estime pas moins qu'il demeure nécessaire d'améliorer la protection des droits humains dans la proposition, sans pour autant porter atteinte à la défense des intérêts légitimes de l'État en matière de sécurité et d'ordre publics. L'enjeu du contrôle des mesures de lutte contre le terrorisme, le radicalisme, la criminalité organisée et l'espionnage est essentiel pour la défense des droits individuels. L'Institut formule donc huit recommandations destinées à renforcer les garanties pour le droit à la vie privée, le droit au recours effectif et les autres droits humains concernés :

1. Le fait que l'utilisation des méthodes exceptionnelles mentionnées dans les articles 18/11, 18/13, 18/15 et 18/16 de la loi organique n'entraîne pas d'obligation de notification active doit être justifié. En l'absence d'une telle justification, ces méthodes exceptionnelles devraient également entrer dans le champ d'application de la modification législative.
2. Dans l'article 2 proposé, qui remplace l'article 2, §3 de la loi organique, la première condition de l'obligation de notification active devrait être reformulée comme suit : "1° la notification ne causera pas de préjudice grave et raisonnablement prévisible à ladite enquête".
3. Dans l'article 2 proposé, qui remplace l'article 2, §3 de la loi organique, la troisième condition de l'obligation de notification active devrait être reformulée comme suit : "3° la notification ne cause pas de préjudice grave et raisonnablement prévisible aux relations que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales."
4. Les exceptions à l'obligation de notification active prévues doivent être interprétées de manière stricte, et un contrôle rigoureux de l'application des exceptions par la Commission BIM et le Comité permanent R est nécessaire. Des critères supplémentaires d'application devraient être élaborés à cette fin.
5. La personne qui a fait l'objet d'une méthode exceptionnelle de collecte de données doit en être informée le plus tôt possible. La notification doit avoir lieu dès qu'il est clair qu'aucune des exceptions ne s'applique, et un premier examen de la possibilité de notifier doit avoir lieu au plus tard un an après la fin de la méthode utilisée.
6. Lorsque la personne qui a fait l'objet d'une méthode exceptionnelle ne peut être jointe, l'impossibilité de notification doit être signalée à la Commission BIM et au Comité permanent R, en exposant les circonstances qui ont rendu la notification impossible. Cela permettra de vérifier que tous les efforts raisonnables ont été entrepris pour effectuer la notification.
7. La notification doit également indiquer exactement quel lieu non accessible au public a fait l'objet de la méthode de récolte de données et, en tout état de cause, doit mentionner explicitement les voies de recours dont dispose la personne qui a fait l'objet de cette méthode exceptionnelle.
8. Il faut inscrire dans la loi un recours a posteriori permettant de contester la légalité et la proportionnalité des mesures exceptionnelles de surveillance adoptées. Ce recours pourrait être de nature indemnitaire et forfaitaire, et devrait soit permettre l'effacement des données détenues par les services de renseignement et de sécurité soit permettre le dépôt de la décision de justice au dossier. Les décisions doivent par principe être rendues publiques.