



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Gemeinsam Äntwert vum Här Premierminister, Staatsminister, vun der Madamm Justizministesch a vum Här Minister fir bannenzeg Sécherheet op d'parlamentaresch Fro n°7867 vum 5. Abrëll 2023 vum honorabelen Deputéierte Sven Clement

D'Regierung huet der Europäescher Kommissioun folgend Äntwerten op hire Questionnaire ginn:

« 1. For what purpose is the use of spyware permitted under national law:

a. criminal law enforcement?

L'article 88-1 du Code de procédure pénale accorde le pouvoir au juge d'instruction d'ordonner, dans des circonstances exceptionnelles, pour des infractions graves et sous un contrôle très strict, l'utilisation de moyens techniques,

1° de surveillance et du contrôle des télécommunications ainsi que de la correspondance postale ;

2° de la sonorisation et de la fixation d'images de certains lieux ou véhicules ;

3° de la captation de données informatiques.

Les mesures prévues à l'endroit de l'article 88-1 du Code de procédure pénale ne peuvent être ordonnées par le juge d'instruction uniquement et exclusivement dans le cadre de faits d'une gravité particulière emportant une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à deux ans d'emprisonnement, et à l'encontre de personnes poursuivies pour des actes de terrorisme et de financement de terrorisme ainsi que pour des crimes et délits contre la sûreté de l'Etat.

b. national security?

Oui – veuillez vous référer à la réponse à la question 3.

c. any other purpose (please specify)?

/

2. Please list all authorities which are permitted by national law to use or authorise the use of spyware.

a) La police grand-ducale après ordonnance du juge d'instruction conformément à l'article 88-1 du Code de procédure pénale.

b) *Le Service de renseignement de l'État en vertu de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État*¹.

3. If your reply to question 1 b) is affirmative, please specify:

a. the definition of national security or the criteria used to define the scope of national security;

b. the relevant legislation that governs the processing of data for national security purposes;

c. which bodies supervise the use of spyware by public authorities (e.g. internal oversight within national security authorities; external oversight by administrative bodies, independent authorities, courts or the national parliament, etc.).

La loi précitée du 5 juillet 2016 définit clairement la mission du Service de renseignement de l'État (SRE) et délimite également de manière précise le contexte dans lequel celle-ci pourra s'exercer : la présence d'une menace ou d'un risque de menace pour la sécurité nationale, à savoir une activité susceptible de mettre en cause l'indépendance et la souveraineté de l'État, la sécurité et le fonctionnement des institutions, les droits fondamentaux et les libertés publiques, la sécurité des personnes et des biens, le potentiel scientifique et technique ou les intérêts économiques du Grand-Duché de Luxembourg. Le champ d'application de cette mission s'étend aussi à la sécurité des États étrangers ou des organisations internationales et supranationales avec lesquelles le Luxembourg a signé des accords.

La loi précise la nature des menaces potentielles pour la sécurité nationale:

- *espionnage et ingérence;*
- *extrémisme à propension violente;*
- *terrorisme;*
- *prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies afférentes;*
- *crime organisé et cyber-menace dans la mesure où ils se trouvent liés à l'une des menaces précédentes*

Il importe de souligner que la loi précitée exclut explicitement de la mission du SRE toute surveillance politique interne.

Par ailleurs, pour garantir une sécurité juridique aussi bien aux citoyens qu'aux professionnels du renseignement, le SRE est soumis à un contrôle à quatre niveaux, dont trois se situent en amont (niveau politique, niveau administratif et autorités judiciaires) et un a posteriori (au niveau parlementaire).

¹ <https://legilux.public.lu/eli/etat/leg/loi/2016/07/05/n8/jo>

4. What are the conditions for the use of spyware under question 1 a), 1 b) and 1 c)? Please explain the type of safeguards that exist under national law (e.g. whether there is a limit on what data can be accessed, on the duration of the measure, on the personal scope, etc.).

Ad 1.a)

L'article 88-2 du Code de procédure pénale vise à délimiter le cadre dans lequel le juge d'instruction peut ordonner une des mesures prévues par l'article 88-1 précité.

Les mesures prévues à l'endroit de l'article 88-1 du Code de procédure pénale ne peuvent être ordonnées par le juge d'instruction uniquement et exclusivement dans le cadre de faits d'une gravité particulière emportant une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à deux ans d'emprisonnement, et, s'agissant de la sonorisation et de la fixation d'images des lieux et véhicules visés à l'article 88-1, paragraphe 2, et de la captation de données informatiques, à l'encontre de personnes poursuivies pour des actes de terrorisme et de financement de terrorisme ainsi que pour des crimes et délits contre la sûreté de l'Etat.

En ce qui concerne la sonorisation et de la fixation d'images des lieux et véhicules visés à l'article 88-1, paragraphe 2, précité, et de la captation de données informatiques, en tout ou en partie, il doit s'agir d'un ou de plusieurs des faits énumérés ci-après :

- « a) crimes et délits contre la sûreté de l'État au sens des articles 101 à 123 du Code pénal ;*
- b) actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal ;*
- 2° que des faits déterminés rendent la personne à surveiller suspecte, soit d'avoir commis l'infraction ou d'y avoir participé, soit de recevoir ou de transmettre des informations destinées à l'inculpé ou au suspect ou qui proviennent de lui ;*
- 3° que les moyens ordinaires d'investigation s'avèrent inopérants en raison de la nature des faits et des circonstances spéciales de l'espèce. »*

L'article poursuit que « (3) La décision du juge d'instruction est écrite et contient, sous peine de nullité, les mentions suivantes :

- 1° la motivation spéciale d'après les éléments de l'espèce et par référence aux conditions indiquées au paragraphe 2 ;*
- 2° le nom ou, s'il n'est pas connu, une description aussi précise que possible de la ou des personnes visées par les mesures ordonnées ;*
- 3° la manière dont les mesures seront exécutées ;*
- 4° la période durant laquelle les mesures pourront être exécutées au regard des dispositions du paragraphe 4 ;*
- 5° le nom et la qualité de l'officier de police judiciaire qui procède à l'exécution de l'enquête. »*

L'article 88-2, paragraphe 4, délimite le champ d'application temporel desdites mesures en imposant qu'elles doivent être levées dès qu'elles ne sont plus nécessaires. Elles cessent de plein droit un mois à compter de la date de l'ordonnance. Elles peuvent toutefois être prorogées chaque fois pour un mois, sans que la durée totale puisse dépasser un an, par ordonnance motivée du juge d'instruction, approuvée par le président de la chambre du conseil de la cour d'appel qui statue dans les deux jours de la réception de l'ordonnance, le procureur général d'État entendu en ses conclusions.

La mesure ne peut, à peine de nullité, être ordonnée à l'égard d'un inculpé après son premier interrogatoire par le juge d'instruction et celle ordonnée antérieurement cesse ses effets de plein droit à cette date (article 88-2, paragraphe 5).

L'article 88-2, paragraphe 6, interdit, sous peine de nullité, d'ordonner les mesures précitées à l'égard d'une personne liée par le secret professionnel au sens de l'article 458 du Code pénal, à moins qu'elle ne soit elle-même suspecte d'avoir commis l'infraction ou d'y avoir participé.

Conformément à l'article 88-2, paragraphe 6, alinéa 3, « la mise en place du dispositif technique mentionné aux paragraphes 2 et 3 de l'article 88-1 ne peut, à peine de nullité, être réalisée dans les locaux utilisés à des fins professionnelles, le domicile ou ses dépendances au sens des articles 479, 480 et 481 du Code pénal ou le véhicule d'un avocat, d'un médecin, d'un journaliste professionnel ou d'un éditeur, ces deux derniers termes compris au sens défini par la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias, ou concerner les systèmes automatisés de traitement de données se trouvant dans ces lieux ».

L'article 88-4 précise encore que « les enregistrements des télécommunications, conversation, images ou données informatiques et les correspondances postales interceptées sont détruits, à la diligence du procureur d'État ou du procureur général d'État, à l'expiration du délai de prescription de l'action publique. En cas de décision d'acquiescement, ils sont détruits immédiatement après que la décision est coulée en force de chose jugée. En cas de condamnation, ils ne sont pas détruits. »

Ad 1.b)

La mise en œuvre des moyens et mesures de recherche prévus aux articles 7(1), 7(2) et 8 (1)c de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État est soumise à des conditions strictes et à des critères précis. La mise en œuvre doit être conforme à trois principes essentiels, qui sont la légitimité, la proportionnalité et la subsidiarité. Cette démarche vise à allier professionnalisme dans la prévention de menace à un haut niveau de protection de l'individu et de sa sphère privée.

Les mesures doivent ainsi viser des personnes physiques ou morales, identifiées ou identifiables.

La surveillance et le contrôle des télécommunications (article 7(1) de la Loi SRE) est limitée à un délai de 3 mois à compter du jour où elle a été ordonnée par le Comité ministériel, après

assentiment de la commission spéciale de magistrats, sur demande écrite du directeur du SRE. Elle peut être renouvelée dans les mêmes conditions de forme et de fond.

La mesure cesse également en cas de transmission du dossier au procureur d'Etat compétent dans les limites des faits communiqués.

La mesure de repérage des données relatives au trafic, y compris l'identification des correspondants, et de toutes les formes de communication, ou à la localisation de l'origine ou de la destination de ces communications (article 7(2) de la Loi SRE) est limitée à une période maximale de 6 mois précédant ou suivant la date à laquelle elle a été ordonnée par le Comité ministériel, après assentiment de la commission spéciale de magistrats, sur demande écrite du directeur du SRE.

Elle peut être renouvelée dans les mêmes conditions de forme et de fond.

La mesure d'interception à la source visée à l'article 8(1)c de la Loi SRE obéit aux mêmes principes précités, et est soumise aux conditions cumulatives suivantes :

- les moyens et mesures de recherche dont dispose le SRE en vertu des articles 5,6, et 7, s'avèrent inopérants en raison de la nature des faits et des circonstances spécifiques de l'espèce*
- Il s'agit d'un ou plusieurs faits qui revêtent un degré de gravité caractérisé*
- les faits ont trait soit à des activités d'espionnage, soit à des activités de prolifération d'armes de destruction massive ou de produits liés à la défense et de technologies y afférentes, soit à des activités de terrorisme.*

La mesure permet d'accéder au(x) système(s) informatique(s) susceptible(s) d'être utilisé(s) par une personne ou plusieurs personnes visées par les moyens et mesures de recherche, afin de

- rechercher de manière ciblée des renseignements nécessaires à l'exécution d'une des missions définies au premier alinéa ou de*
- surveiller et contrôler des communications dont l'interception technique n'est pas possible moyennant les réseaux normaux de télécommunication et à ce titre y installer un dispositif technique ou informatique non permanent d'une durée n'excédant pas le délai de trois mois.*

Les moyens et mesures de recherche susvisés sont ordonnés par le Comité ministériel sur demande écrite du directeur du SRE et après l'assentiment de la commission spéciale selon la procédure inscrite à l'article 7.

5. Please specify if the use of spyware for purposes under question 1 a), 1 b) and 1 c) requires prior authorisation by a court or an independent administrative authority. If yes, please explain:

a. the circumstances where prior authorisation is required and any criteria allowing the authorisation to be issued;

b. which court or independent administrative authority provides the authorisation;

c. whether the court or the independent administrative authority has access to all information relating to the request for prior authorisation.

Ad 1.a)

Veillez vous référer aux réponses aux questions 1.a) et 4.

Ad 1.b)

Les moyens et mesures de recherche prévus aux articles 7-8 de la loi précitée du 5 juillet 2016 sont ordonnés par le Comité ministériel du renseignement, composé de membres du Gouvernement, sur demande écrite du directeur du SRE et après l'assentiment d'une commission spéciale composée de magistrats, à savoir le président de la Cour supérieure de justice, le président de la Cour administrative et le président du tribunal d'arrondissement de Luxembourg.

6. Are there any transparency requirements with respect to the use of spyware (e.g. reporting obligations to Parliament or oversight bodies on the use of spyware, public reporting on statistics, etc.)? Please specify the transparency requirements under question 1 a), 1 b) and 1 c).

La mesure de la captation de données informatiques ne peut être ordonnée uniquement dans l'exercice des missions de protection de la sécurité nationale et de la sûreté de l'État et dans le cadre d'un dispositif de contrôle strictement réglementé.

Il importe également de rappeler que la loi du 1^{er} août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale s'applique également à la Police grand-ducale.

Les activités du Service de renseignement de l'État sont soumises au contrôle d'une commission de contrôle parlementaire. La commission de contrôle parlementaire est informée d'office tous les six mois des mesures de surveillance et de contrôle des communications ordonnées par le comité ministériel du renseignement, à la demande du SRE.

7. Please specify:

a. whether there is any requirement to notify the concerned individual(s), once there is no longer a risk to national security;

b. what remedies are available to an individual who was subject to surveillance by means of spyware (e.g. judicial redress, administrative redress such as lodging a complaint to ombudspersons or oversight bodies);

c. whether the administrative or judicial remedy examines the lawfulness of such a measure including whether the purposes specified in question 1 were invoked legitimately.

Conformément à l'article 88-4, paragraphe 6, du Code de procédure pénale, « [l]a personne surveillée par un moyen technique au sens de l'article 88-1, paragraphe 1^{er}, (...) sont, pour autant qu'ils n'ont pas la qualité d'inculpé ou de partie civile, informés par le juge d'instruction de la mesure ordonnée ainsi que de leur droit de former un recours en nullité sur base et dans les conditions de l'article 126 au moment de la dernière inculpation intervenue dans l'instruction préparatoire en question ou, lorsque l'instruction préparatoire est clôturée par le juge d'instruction sans inculpation, au moment de cette clôture. »

Puis, le paragraphe 7 de l'article 88-4 du Code de procédure pénale permet au procureur d'Etat de « former appel dans tous les cas des ordonnances du juge d'instruction conformément à l'article 133 ».

Concernant le SRE, l'autorité de contrôle instituée par l'article 3 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données est compétente pour contrôler et vérifier le respect par le SRE des dispositions légales, en vertu de l'article 39 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

L'article 13 de la loi précitée règle le droit d'accès par la personne concernée. Ainsi cette personne a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées. Selon l'article 14, le responsable du traitement peut néanmoins limiter, entièrement ou partiellement, le droit d'accès de la personne concernée, notamment afin de protéger la sécurité nationale. En outre, la personne concernée a le droit de demander la rectification ou l'effacement des données à caractère personnel relatives à elle, ainsi que la limitation du traitement de ces données (art. 15) en cas d'inexactitude de données, ou de violations de dispositions légales inhérentes à la protection des données personnelles, ou de respect d'une obligation légale pour le responsable de traitement.

En vertu de l'article 16, les droits de la personne concernée peuvent être exercés par l'intermédiaire de l'autorité de contrôle compétente, à savoir la Commission nationale pour la protection des données (CNPD). »

Lëtzebuerg, den 28. Abrëll 2023

De Premierminister, Staatsminister

(s.) Xavier BETTEL