N° 6921[1]

CHAMBRE DES DEPUTES

Session ordinaire 2015-2016

P R O J E T D E L O I

portant:

1) modification du Code d'instruction criminelle;

2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel;

3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(12.2.2016)

Conformément à l'article 32 paragraphe (3) lettres (e) et (f) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée „la loi du 2 août 2002"), la Commission nationale pour la protection des données a notamment pour mission de présenter au gouvernement toutes suggestions susceptibles d'améliorer le cadre légal et d'aviser *„tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi"*.

Par lettre du 4 décembre 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6921 portant 1) modification du Code d'instruction criminelle; 2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Ces dernières années, la lutte contre le terrorisme est devenue à la fois cruciale et plus difficile. L'émergence et l'évolution rapide des nouvelles technologies permettent l'utilisation de nouveaux outils de détection et de poursuite. Le projet de loi sous examen s'inscrit ainsi parmi des initiatives similaires des pays limitrophes[1], qui ont estimé nécessaire d'introduire de nouvelles mesures de surveillance pour combattre le terrorisme[2].

La Commission nationale constate que les moyens d'investigation proposés élargissent les pouvoirs du procureur d'Etat, du juge d'instruction et de la police judiciaire et facilitent la consultation, la conservation et l'utilisation d'une pléthore de données à caractère personnel. Ces mesures ont ainsi un impact considérable sur les droits fondamentaux des citoyens, notamment le droit à la vie privée et le droit à la protection des données à caractère personnel, consacrés dans l'article 8 de la Convention européenne des droits de l'homme et dans les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Conformément à ces textes, une limitation de ces droits fondamentaux doit être prévue par la loi et les mesures doivent être nécessaires dans une société démocratique pour atteindre un but légitime. Il découle de la jurisprudence de la Cour européenne des droits de l'homme, ainsi que de celle de la Cour

---

1 Tels que la Belgique, la France, l'Allemagne et les Pays-Bas.

2 La Cour européenne des droits de l'homme a également constaté la nécessité de mesures de surveillance secrète. Voir l'arrêt *Klass et autres c. Allemagne*, 6 septembre 1978, § 48, série A n° 28.

de justice de l'Union européenne qu'une telle ingérence doit impérativement être limitée à ce qui est strictement nécessaire dans une société démocratique[3]. Plus particulièrement, elle doit être proportionnée au but légitime poursuivi. Ceci implique que la loi doit établir des critères objectifs encadrant et limitant la collecte et l'utilisation des données à caractère personnel par les autorités répressives[4].

La loi doit en outre être accessible et suffisamment claire et précise pour permettre aux citoyens de savoir en quelles circonstances et sous quelles conditions ces mesures peuvent être mises en oeuvre, ainsi que de connaître les conséquences éventuelles pour eux[5]. Il est nécessaire que la loi définisse avec une clarté suffisante l'étendue et les modalités d'exercice des pouvoirs conférés aux autorités compétentes, ainsi que les garanties aptes à protéger efficacement les données à caractère personnel[6].

De plus, l'exercice des pouvoirs doit être soumis à un contrôle par un organe indépendant, telle qu'une juridiction ou une autorité administrative indépendante, afin de limiter le risque d'abus[7]. D'après la Cour européenne des droits de l'homme, dans le cadre des mesures de surveillance, c'est *„en principe souhaitable que le contrôle soit confié à un juge 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"*[8].

Finalement, il faut que la loi prévoie des voies de recours pour les personnes ayant fait l'objet d'une mesure de surveillance[9]. En effet, en introduisant des mesures limitant les droits fondamentaux des citoyens, il faut obligatoirement qu'un juste équilibre soit ménagé entre le respect de ces droits et l'intérêt public de détecter et poursuivre les infractions pénales[10].

Dans ce sens, la Commission nationale s'interroge sur les circonstances dans lesquels ces nouveaux outils d'investigation pourront être mis en oeuvre. Le projet de loi, qui s'inscrit dans le contexte des menaces et attentats terroristes récents dans nos pays voisins, décrit dans l'introduction de l'exposé des motifs la nécessité de mettre à jour la législation luxembourgeoise afin de pouvoir combattre efficacement le terrorisme. Or, le texte sous examen ne se limite pas à cet objectif unique. Il étend le champ d'application de l'article 24-1 aux „crimes flagrants" et introduit la mesure prévue à l'article 48-27 projeté à la poursuite de tous crimes et délits, peu importe qu'il s'agisse ou non d'actes de terrorisme. La Commission nationale regrette que l'objectif de faciliter, en général, la poursuite de tous crimes et délits n'est pas clairement séparé de l'objectif principal du projet de loi, qui est la mise en place de nouveaux moyens d'investigations pour lutter plus efficacement contre le terrorisme.

La Commission nationale note finalement qu'en décembre 2015, le Parlement européen et le Conseil sont arrivés à un accord informel sur le texte de la Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données[11].

Le texte de compromis du projet de directive reprend les grands principes en matière de protection des données et y ajoute des obligations pour garantir que les données à caractère personnel soient protégées du début jusqu'à la fin de la procédure pénale. Le texte de compromis du projet de directive

---

3 *Klass et autres c. Allemagne*, 6 septembre 1978, § 48, série A n° 28; *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et 30566/04, § 101, CEDH 2008-V; *Szabo et Vissy c. Hongrie*, n° 37138/14, § 53, 12 janvier 2016.

4 *Arrêt Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, point 39; Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 94.

5 Voir entre autres: *Liberty et autres c. Royaume-Uni*, n° 58243/00, § 59-62, 1er juillet 2008 et les jurisprudences citées; *Zakharov c. Russie* [GC], n° 47413/06, § 228-229, 4 décembre 2015.

6 Voir entre autres: *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et 30566/04, § 95 et 103, CEDH 2008-V; *Liberty et autres c. Royaume-Uni*, n° 58243/00, § 59-62, 1er juillet 2008 et les jurisprudences citées; *Zakharov c. Russie* [GC], n° 47413/06, § 230-231, 4 décembre 2015; Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 91 et jurisprudences citées.

7 *Klass et autres c. Allemagne*, 6 septembre 1978, § 51-57, série A n° 28: *Szabo et Vissy c. Hongrie*, 37138/14, § 77, 12 janvier 2016.

8 *Klass et autres c. Allemagne*, 6 septembre 1978, § 56, série A n° 28. Voir aussi *Szabo et Vissy c. Hongrie*, n° 37138/14, § 77, 12 janvier 2016; Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 95.

9 Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 94.

10 Voir notamment *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et 30566/04, § 112, CEDH 2008-V.

11 Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, et à la libre circulation de ces données, 2012/0010 (COD), texte de compromis datant du 15 décembre 2015.

dispose que les Etats Membres doivent prévoir des délais pour l'effacement des données ou une révision périodique de la nécessité de conserver celles-ci[12], instaurer des principes de la protection des données dès la conception et de la protection des données par défaut (*data protection by design and data protection by default*)[13] et veiller à ce que des techniques de journalisation soient utilisées pour une série de traitements[14].

Au vu de ce qui précède, la Commission nationale tient à souligner l'importance de la conformité du présent projet de loi avec les principes régissant la protection des données en général et avec le texte de compromis du projet de directive en particulier.

Ci-dessous seront passés en revus les articles que le projet de loi sous avis propose d'ajouter à la législation luxembourgeoise ou de modifier.

*

1. LA TERMINOLOGIE

A titre préliminaire, la Commission nationale constate que les termes utilisés dans le projet de loi ne correspondent pas à ceux figurant dans la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électronique („loi du 30 mai 2005"), qui transpose plusieurs directives européennes. En effet, dans le projet de loi, il est question d'„opérateurs et fournisseurs de communications électroniques" alors que la loi du 30 mai 2005 fait état d'opérateurs (de réseau) et de fournisseurs de services (de communications électroniques). De plus, la loi du 30 mai 2005 parle de communications électroniques et non de télécommunications.

La Commission nationale recommande dès lors d'aligner la terminologie du projet de loi (ainsi que celle des articles 24-1 et 67-1 actuels du Code d'instruction criminelle) sur celle d'ores et déjà utilisée dans la législation européenne et nationale.

*

2. ARTICLE 24-1 DU CODE D'INSTRUCTION CRIMINELLE

Le projet de loi prévoit de permettre le repérage ou la localisation de communications électroniques en cas de crime flagrant avant qu'une instruction préparatoire ne soit ouverte.

Le projet de loi, en son état actuel, appelle les observations suivantes:

2.1. Les infractions visées

A l'avenir, l'article 24-1 du Code d'instruction criminelle permettra le repérage ou la localisation de communications électroniques *„pour les crimes flagrants"*. Il est sous-entendu que ces mesures pourront être ordonnées pour *tous* types de crimes.

Dans ce contexte, il y a lieu de rappeler que l'article 24-1 prévoit un accès aux données de communications conservées en vertu des articles 5 et 9 de la loi du 30 mai 2005.

Ce type de conservation des données de connexion de communications électroniques est au centre de l'arrêt de la Cour de justice de l'Union européenne (ci-après la CJUE) rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12.

Il résulte dudit arrêt[15] que l'accès par les autorités judiciaires à de telles données doit être délimité de manière très précise, notamment pour ce qui est des infractions permettant un tel accès. Il faudrait vérifier en détail quelles sont les infractions pour lesquelles la commission justifie cet accès eu égard à l'ampleur et à la gravité de l'ingérence dans les droits fondamentaux consacrés par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne.

---

12 Ibid., Article 4b et considérant 18.

13 Ibid., Article 19.

14 Ibid., Article 24.

15 Cf. notamment le considérant 60 de l'arrêt.

Le projet de loi n° 6763[16] a justement comme objectif de mettre la législation luxembourgeoise en conformité aux principes énoncés dans l'arrêt précité de la CJUE et à cette fin notamment d'établir une liste des infractions visées.

Afin que la charte des droits fondamentaux de l'Union européenne et l'arrêt de la CJUE du 8 avril 2014 soient respectés, il conviendrait d'établir d'abord ce catalogue d'infractions avant d'étendre les possibilités de repérage et traçage existantes à tous crimes flagrants.

2.2. La protection des personnes titulaires d'un secret professionnel et des journalistes

Le fait de pouvoir retracer toutes sortes de communications électroniques de quiconque permet de savoir quelles ont été les personnes ayant été en contact avec des personnes titulaire d'un secret professionnel, tels que les avocats, médecins etc., et avec les journalistes qui bénéficient d'une protection légale de leurs sources.

La législation luxembourgeoise ne prévoit aucune exception pour ce qui est des communications soumises au secret professionnel, ni au niveau de la conservation des données de communications (articles 5 et 9 de la loi du 30 mai 2005), ni au niveau de l'accès aux données par les autorités judiciaires (articles 24-1 et 67-1 du Code d'instruction criminelle).

Rappelons dans ce contexte que la directive 2006/24/CE a été déclarée invalide notamment en raison du fait qu'elle ne prévoyait *„aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel"*.

Par ailleurs, il se pose la question de savoir si le secret des sources des journalistes, qui a fait l'objet d'une jurisprudence abondante de la part de la Cour européenne des droits de l'homme, est suffisamment protégé.

Certes, la loi du 8 juin 2004 sur la liberté d'expression dans les médias prévoit la protection des sources des journalistes. On peut cependant se demander si cette protection satisfait aux exigences de la prédite jurisprudence de Strasbourg[17].

La Commission nationale a d'ailleurs rendu attentif le législateur à ces lacunes de la législation luxembourgeoise dans le contexte du projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques[18].

En l'état, la Commission nationale estime que le texte du projet de loi ne répond pas aux exigences de la jurisprudence européenne.

2.3. Raison d'être de l'extension du champ d'application de l'article 24-1 alinéas 3 et suivants

Selon le commentaire des articles, l'extension projetée permettra un traçage ou une localisation à un stade très précoce des investigations. A l'heure actuelle, une instruction ne pourrait guère être ouverte, car *„le juge d'instruction ne pourra pas être saisi sur base d'un dossier d'enquête tant soit peu complet."*

En ordonnant un traçage ou une localisation sur base de l'article 24-1, le juge d'instruction est toujours censé apprécier si la mesure est nécessaire à la manifestation de la vérité et rendre une ordon-

---

16 Projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

17 Pour un cas de figure postérieur à la loi du 8 juin 2004: voir l'arrêt de la Cour européenne des droits de l'homme (Cinquième section) du 18 avril 2013 rendu dans l'affaire Saint-Paul Luxembourg S.A. c. Luxembourg, requête n° 26419/10.

18 Avis n° 214/2014 du 13 mai 2014 (Avis de la Commission nationale pour la protection des données quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication); Avis n° 228/2015 du 19 juin 2015 (Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques).

nance motivée indiquant les circonstances de l'espèce. La Commission nationale présume en effet que les conditions de l'67-1 sont également applicables à une mesure ordonnée sur base de l'article 24-1[19].

Si la Commission nationale a toujours insisté sur la nécessité d'une décision judiciaire en matière d'accès aux données de trafic de communications électroniques, encore faut-il que les conditions soient réunies pour que l'appréciation judiciaire fonctionne bien en pratique[20].

Il est très difficile d'apprécier, si, en l'espèce, les juges saisis seront toujours en mesure de bien apprécier en connaissance de cause, alors qu'ils sont censés trancher à un moment où le dossier de l'enquête est encore peu complet.

En ce qui concerne l'autre motif invoqué dans le commentaire des articles pour l'extension, à savoir la gestion de crise en cas de crime qui se poursuit comme par exemple en cas de prise d'otage, il concerne certainement seulement un petit pourcentage des affaires. Dès lors, une mesure ciblée pour ces cas de figure serait plus justifiée qu'une extension généralisée du champ d'application de l'article 24-1.

2.4. Conclusion

La Commission nationale ne rejette pas, *a priori*, l'idée d'une telle extension si, comme prévu en l'espèce, cette mesure ne se fait que sur ordonnance d'un juge d'instruction, que l'extension soit précédée par un catalogue d'infraction, limitée à des mesures ciblées et réponde aux exigences de la jurisprudence européenne.

*

3. ARTICLE 39 DU CODE D'INSTRUCTION CRIMINELLE

La Commission nationale n'a pas d'observations à faire concernant cet article.

*

4. ARTICLE 48-26 DU CODE D'INSTRUCTION CRIMINELLE

L'article 48-26 nouveau a pour objet d'introduire en droit luxembourgeois l'enquête sous pseudonyme.

4.1. Les personnes surveillées

L'article 48-26 du projet de loi prévoit la possibilité pour les officiers de police judiciaire de procéder à des enquêtes sous pseudonyme dans le but de constater des crimes et délits contre la sûreté de l'Etat ou des actes de terrorisme et de financement de terrorisme. Serait, par exemple, possible a) la participation sous un pseudonyme aux échanges électroniques, b) le contact, sous un pseudonyme, avec les personnes susceptible d'être les auteurs de ces infractions et c) l'extraction, l'acquisition ou la conservation par ce moyen des éléments de preuve et des données sur les personnes susceptibles d'être les auteurs des infractions. Ces mesures permettraient en conséquence aux officiers de police judiciaire de s'intégrer dans des communautés virtuelles et ainsi recueillir de nombreuses informations sur des personnes présumées être les auteurs des infractions sur lesquelles porte l'enquête.

Par ailleurs, comme l'a souligné un arrêt de la cour constitutionnelle allemande sur la *„cyber-infiltration"* et la captation des données informatiques, non seulement les données de la personne surveillée peuvent être traitées, mais également celles de toutes les personnes avec qui la personne surveillée

---

19 L'avis de la Commission nationale n'a d'ailleurs pas été demandé lors de l'introduction des alinéas 3 et suivants de l'article 24-1 du Code d'instruction criminelle en 2014.

20 Voir à ce sujet: Astrid Ackermann, *„Funktioniert der Richtervorbehalt?"*, 26 août 2015. Disponible sur „https://www.datenschutzbeauftragter-info.de/funktioniert-der-richtervorbehalt/".

entre en contact[21]. Par exemple, en s'inscrivant à un forum de discussion, l'officier de police judiciaire pourra consulter les données à caractère personnel de chaque utilisateur du forum.

Rappelons que selon l'article 2 lettre (r) de la loi du 2 août 2002 et l'article 3(3) du texte de compromis du projet de directive, la simple consultation est considérée comme un traitement de données à caractère personnel. La consultation ou l'utilisation des données relatives à n'importe quel membre d'un forum de discussion constituerait dès lors un traitement de données à caractère personnel au sens de la loi et non seulement les données relatives aux personnes susceptibles d'être les auteurs de ces infractions. Or, conformément à l'article 4 paragraphe (1) lettre (b) de la loi du 2 août 2002, les données à caractère personnel doivent être *„adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées …"*[22].

La Commission nationale se rallie au groupe de travail „Article 29" qui a souligné que le traitement des données à caractère personnel relatives aux personnes non soupçonnées d'avoir commis une infraction *„ne devrait être autorisé que dans certaines conditions spécifiques et pour autant qu'il soit absolument nécessaire à une finalité légitime, clairement définie et particulière"*[23]. Le traitement des données à caractère personnel relatives aux personnes non soupçonnées d'avoir commis une des infractions figurant dans l'article 48-26 du projet de loi devrait en conséquence se limiter à ce qui est strictement nécessaire.

Afin de limiter le traitement de ces données et d'assurer la conformité de l'article à la loi du 2 août 2002, la Commission nationale recommande au législateur de s'inspirer de l'article 48-17 paragraphe (5) du Code d'instruction criminelle relatif à l'infiltration et d'instaurer une obligation expresse pour l'officier de police judiciaire qui a effectué l'enquête de consigner dans son rapport seulement les données strictement nécessaires à la constatation des infractions et d'omettre toutes données à caractère personnel relatives à des personnes non susceptibles d'être les auteurs des infractions.

4.2. La limitation des personnes pouvant procéder à l'enquête sous pseudonyme

Le projet de loi autorise tout officier de police judiciaire de procéder à des enquêtes sous pseudonyme. En revanche, d'après l'article 706-87-1 du Code de procédure pénale français, dont s'inspire l'article 48-26 du projet de loi, cette mesure ne peut être mise en oeuvre que par les officiers ou agents de police judiciaire qui *„sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin"*.

Conformément à la jurisprudence de la CJUE et de la Cour européenne des droits de l'homme, les dispositions limitant le droit à la protection des données à caractère personnel doivent contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées *„contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données"*[24]. Une telle protection pourrait être assurée en limitant *„le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi"*[25].

Au vu de ce qui précède, la Commission nationale considère que le projet de loi sous examen devrait limiter le nombre des personnes pouvant procéder à des enquêtes sous pseudonyme à des officiers de police judiciaire spécialement habilités à cette fin, à l'instar de l'article 706-87-1 du Code de procédure pénale français.

---

21 BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 – Rn. (1-333), § 297 *„Betroffen ist nicht nur derjenige, der den Anlass für die Überwachungsmaßnahme gegeben hat. Der Eingriff kann vielmehr eine gewisse Streubreite aufweisen, wenn Erkenntnisse nicht nur über das Kommunikationsverhalten desjenigen, gegen den sich die Maßnahme richtet, sondern auch über seine Kommunikationspartner gewonnen werden."*.

22 Cette condition est reprise dans l'article 4 paragraphe (1) lettre (c) du texte de compromis du projet de directive, qui prévoit que *„Member States shall provide that personal data must be … adequate, relevant, and not excessive in relation to the purposes for which they are processed …"*.

23 GA29, *Avis 03/2015*, 1er décembre 2015, p. 7; GA29, *Avis 01/2013*, 26 février 2013, p. 3.

24 *S et Marper c. Royaume-Uni* [GC], n° 30562/04 et 30566/04, § 99 et 103, CEDH 2008-V; Affaires jointes CE293/12 et C-594/12, *Digital Rights Ireland* e.a.. ECLI:EU:C:2014:238, considérant 54.

25 Voir par rapport à la conservation des données à caractère personnel, les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland* e.a., ECLI:EU:C:2014:238, considérant 62.

4.3. La nature du pseudonyme utilisé

Par ailleurs, le projet de loi ne contient aucune précision quant aux pseudonymes qui pourront être utilisés par les officiers de police judiciaire, notamment s'il s'agit des identités fictives ou des identités „réelles". Etant donné que l'utilisation d'une identité „réelle" pourrait causer des graves préjudices aux personnes dont les identités seraient usurpées, la Commission nationale estime nécessaire de préciser que les officiers de police judiciaire ne pourront en aucun cas avoir délibérément recours à des identités „réelles".

4.4. Conclusion

Dans un souci de limiter la collecte de données et d'assurer la conformité de l'article aux principes fondamentaux du droit des individus à la protection de leurs données, la Commission nationale recommande aux auteurs du projet d'y apporter les limitations développées ci-avant.

Finalement, d'un point de vu rédactionnel, la Commission nationale suppose que les infractions énumérées dans l'article 48-26 paragraphe (2) alinéa 2 devraient être „les actes *de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6*, …", et non *„les actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 136-6, …"*.

*

5. ARTICLE 48-27 DU CODE D'INSTRUCTION CRIMINELLE

Ce nouvel article est appelé à permettre au procureur d'Etat ou au juge d'instruction de requérir les opérateurs de télécommunications et les fournisseurs d'un service de télécommunications d'identifier l'abonné ou l'utilisateur habituel de leurs services ou d'identifier les services auxquels une personne donnée est abonnée ou qu'elle utilise habituellement.

5.1. Articulation de l'article

La disposition est formulée en des termes généraux ce qui pourrait ne pas satisfaire à l'exigence de clarté et de prévisibilité posée par la jurisprudence de la Cour européenne des droits de l'homme. La Commission nationale se pose par ailleurs des questions quant à l'articulation de l'article sous avis par rapport à d'autres dispositions existantes et à adopter.

Si la Commission nationale adopte une lecture restrictive des éléments pouvant être identifiés aux termes de cet article, à savoir l'identité seule de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé d'une part, et celle des services de communication électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, d'autre part, ce qui selon sa compréhension exclut expressis verbis le retracement des données de trafic et de localisation relatives aux communications électroniques, elle s'étonne toutefois du libellé de l'article 41, qui bien que n'étant qu'un biais par lequel l'art. 48-27 peut être mise en oeuvre, semble néanmoins aller plus loin pour ce qui est de l'étendue des données pouvant être identifiées, alors que leurs libellés diffèrent.

Le projet prévoit en effet que l'accès aux données pourra se faire:

– sur la base de toutes données détenues par le procureur d'Etat ou le juge d'instruction

  ou

– au moyen d'un accès aux fichiers de clients du fournisseur de services ou de l'opérateur

  ou

– sur base de l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

L'accès aux données de trafic des communications étant encadré par l'article 67-1 du Code d'Instruction criminelle et par les dispositions de la loi du 30 mai 2005, on peut en effet exclure que les auteurs du projet de loi ait voulu faire double emploi en prévoyant à nouveau l'accès à cette catégorie de données par le biais de l'article 48-27.

La loi du 30 mai 2005 énumère de manière détaillée en son article 7 paragraphe (5) les données relatives à l'identification.

Ainsi sont visées: *„le numéro de téléphone, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, lieu d'établissement de l'abonné et de l'utilisateur, pour autant que ce dernier soit identifié ou identifiable"*.

Dans un souci d'éviter toute confusion quant à la nature des données d'identification visées par l'article 48-27, la Commission nationale estime nécessaire de reprendre cette énumération dans le corps de texte dudit article.

Pour ce qui est de l'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, la Commission nationale recommande d'adopter une terminologie identique pour les articles 48-27 et 41.

Il est compréhensible, que le législateur veuille procurer aux autorités répressives un moyen d'accéder aux données d'identification des utilisateurs et des moyens de télécommunications que ce dernier utilise, sans devoir recourir aux dispositions de l'article 5 de la loi du 30 niai 2005.

Il est moins compréhensible que pour ce faire, les autorités publiques aient un accès direct à des fichiers privés des sociétés, ce qui constituerait un précédent. Cette nouvelle mesure très intrusive paraît disproportionnée par rapport au but recherché.

Il y a lieu de se demander si un accès sur la base de toutes données détenues par le procureur d'Etat ou le juge d'instruction ou le recours à l'article 41, tel que prévu par le présent projet de loi, ne suffisent pas pour atteindre le but recherché. La Commission nationale suggère dès lors de supprimer du texte du projet de loi la possibilité d'avoir un accès direct aux fichiers des opérateurs.

Les officiers de police judiciaire peuvent, en cas d'urgence, avoir accès aux données visées par l'article 48-27 par les mêmes moyens.

La Commission nationale regrette que l'exposé des motifs et le commentaire des articles soient muets sur la définition de l'extrême urgence, alors que des explications complémentaires auraient pu éclairer la raison pour laquelle l'officier de policier judiciaire se voit doter de si larges compétences, dont notamment l'accès direct à des fichiers. Comment serait d'ailleurs organisé un tel accès direct? La Commission nationale réitère ses doutes quant à la proportionnalité et la nécessité de cette mesure en présence des autres moyens d'accès aux données existantes ou prévues, dont notamment l'article 41 qui permet d'atteindre le même but recherché.

5.2. Appréciation et conclusion

Dans ce contexte, il ne faut pas oublier, que les communications électroniques occupent une place tout-à-fait particulière dans notre Etat de droit. En témoignant notamment:

– la jurisprudence de la Cour européenne des droits de l'homme des dernières des dernières décennies et l'arrêt de la CJUE rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, et
– la législation en matière de protection des données qui accorde une place particulière aux communications électroniques: en effet, il s'agit du seul domaine qui bénéficie d'une législation particulière très développée[26] allant au-delà des règles de droit commun[27] existant en matière de protection des données, et
– le Code d'instruction criminelle qui, par son l'article 67-1, soumet l'accès aux données de trafic de communications électroniques à des conditions plus restrictives que celles s'appliquant aux perquisitions (qu'on pourrait, en quelque sorte, qualifier de „droit commun"):
  • L'accès n'est possible que pour des faits qui emportent une peine criminelle ou une peine correctionnelle, dont le maximum est égal ou supérieur à un an d'emprisonnement.

---

26 La loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques transposant la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

27 La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel transposant la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

- L'accès est soumis à la condition de l'ordonnance du juge d'instruction, et cela même en cas de crime ou de délit flagrant[28].

Dans l'hypothèse du recours à des données relatives au trafic des communications, les autorités judiciaires ont recours aux données conservées en vertu de l'article 5 de la loi du 30 mai 2005.

Il s'agit là du type de conservation de données qui a fait l'objet de l'arrêt de la Cour de justice de l'Union européenne (ci-après la CJUE) rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12.

Le projet de loi n° 6763 a comme objectif de mettre la législation luxembourgeoise en conformité avec l'arrêt précité de la CJUE.

Bien qu'à priori, l'article 48-27 vise beaucoup moins de données (les seules données d'identification) que l'article 5 de la loi du 30 mai 2005 précitée, la Commission nationale constate que le présent projet de loi entend introduire un article qui risque de violer les principes énoncés dans cet arrêt. En effet, l'article projeté est en décalage avec l'arrêt de la Cour sur les points suivants:

– L'accès devrait être réservé aux poursuites concernant les infractions graves clairement déterminées[29]. Or, en l'espèce, il est prévu de permettre l'accès pour tous crimes et délits. Rappelons qu'à l'heure actuelle, l'accès aux données n'est permis que dans le cadre de la poursuite d'infractions dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement et que le projet de loi n° 6763 entend remplacer ce seuil de l'article 67-1 du Code d'instruction criminelle par un catalogue d'infractions.
– Selon la Cour, l'accès aux données devrait être soumis *„à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales"*[30]. Or, l'article 48-27 a justement pour objet de supprimer la nécessité d'une ordonnance préalable écrite d'un juge d'instruction pour un certain nombre d'hypothèses.

Par ailleurs, la limite entre le champ d'application de l'article 67-1 (et de l'article 241) du Code d'instruction criminelle d'un côté et celui du nouvel article 48-27 de l'autre n'est pas claire.

Des cas de figure continuent d'exister pour lesquels, même après l'introduction de l'article 48-27, les mesures resteront soumises aux conditions de l'article 67-1.

Pour le cas où l'article 48-27 devait être maintenu sous sa forme actuelle, la Commission nationale suggère d'amender l'article en y intégrant une liste détaillée et exhaustive des différents types de données censées être soumises dorénavant au champ d'application de l'article 48-27 afin de les distinguer de celles qui resteront soumises exclusivement au champ d'application de l'article 67-1 (et de l'article 24-1), plus protecteur que les nouvelles dispositions projétées.

Encore que la Commission nationale ne saisit pas la réelle plus-value de ce nouveau moyen d'investigation pour les autorités répressives, l'approche choisie par les auteurs du projet de loi lui semble a priori respectueuse des droits fondamentaux des individus et proportionnée au but poursuivi, alors que c'est une approche en deux étapes. D'abord, un accès à des données d'identification est rendu possible

---

28 Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V *„Cette localisation de la provenance de l'appel téléphonique* […] *constitue un repérage de données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, au sens de l'article 67-1 du Code d'instruction criminelle. La compétence pour ordonner un tel repérage appartient en principe au seul juge d'instruction, et ce depuis la loi du 21 novembre 2002 ayant introduit au Code d'instruction criminelle ledit article 67-1. Alors qu'auparavant de telles investigations étaient opérées sur base des articles 65 et 66 du Code d'instruction criminelle, et pouvaient donc également être opérées dans le cadre des crimes et délits flagrants par les officiers de police judiciaire agissant sur base des articles 31 et 33 du Code d'instruction criminelle, le repérage est depuis l'entrée en vigueur de l'article 67-1 réservé à la compétence exclusive du juge d'instruction. Le fait que l'article 67-1 continue à figurer sous la section III „Des transports, perquisitions et saisies", du chapitre 1er du titre III du Livre premier du Code d'instruction criminelle a uniquement pour objet de distinguer le repérage des moyens de surveillance spéciale des télécommunications (articles 88-1 à 88-4 du Code d'instruction criminelle), mais n'autorise pas les officiers de police judiciaire, agissant en vertu des pouvoirs qui leur sont spécialement conférés au titre des crimes et des délits flagrants, à opérer un tel repérage au titre des articles 33 et 31 du Code d'instruction criminelle (perquisition et saisie). L'article 33 du Code d'instruction criminelle est le pendant de l'article 66 du même code, il n'inclut pas les pouvoirs que le juge d'instruction tient de l'article 67-1 dudit code."*

29 Voir à ce sujet le considérant 60 de l'arrêt.

30 Considérant 62 de l'arrêt.

par le biais de l'article 48-27. Pour des enquêtes plus poussées et détaillées, un accès à des données plus sensibles, à savoir les données de trafic des communications et de localisation, est possible en vertu des articles 5 et 9 de la loi du 30 mai 2005.

Or, si contrairement à la lecture que la Commission nationale fait de ce nouvel article, ce dernier devrait tout de même aussi couvrir les données relatifs au trafic des communications et de localisation, elle estime que l'article 48-27 serait manifestement disproportionné par rapport au but recherché, alors qu'il ne contiendrait pas toutes les garanties prévues dans le cadre des articles 5 et 9 de la loi du 30 mai 2005 et de l'article 67-1 du Code d'Instruction criminelle et qu'il s'appliquerait sans distinction à tous crimes et délits et que dès lors, les exigences de la jurisprudence européenne ne seraient pas respectées[31].

Pour des raisons de sécurité et de cohérence juridique, la Commission nationale estime en tout état de cause qu'il y a lieu de coordonner toutes ces dispositions légales éparses existantes et en projet.

5.3. Observations supplémentaires quant à certaines modalités et conditions de l'article 48-27

5.3.1. *Conditions de fond applicables*

La Commission nationale estime que l'accès aux données de communications électroniques ne devrait être permis que s'il est *„nécessaire à la manifestation de la vérité"*, tel que c'est également précisé à l'article 67-1.

5.3.2. *Protection du secret professionnel*

Comme il a déjà été précisé pour l'article 24-1, la Commission nationale estime qu'il conviendrait de prendre des mesures afin de protéger le secret professionnel et le cas échéant le secret des sources des journalistes.

A ce sujet, il est renvoyé aux développements exposés au point 2.2. du présent avis.

5.3.3. *Nullités*

La Commission nationale suggère que l'existence de l'ordonnance et les exigences relatives à sa motivation (devant refléter *„le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête ou d'instruction"*) soient prescrites à peine de nullité.

De même, la condition de l'extrême urgence devrait être prescrite à peine de nullité si la possibilité d'une réquisition par décision d'un officier de police judiciaire en cas d'extrême urgence est maintenue.

*

6. ARTICLE 65 DU CODE D'INSTRUCTION CRIMINELLE

La Commission nationale n'a pas d'observations à faire concernant cet article.

*

7. ARTICLE 88-1 A 88-4 DU CODE D'INSTRUCTION CRIMINELLE

Le projet de loi projette de modifier les articles 88-1 à 88-4 du Code d'instruction criminelle relatives au contrôle des communications afin de mieux définir les mesures susceptibles d'être prises. Au lieu de se tenir à la formule générale et assez vague de *„moyens techniques de surveillance et de contrôle de toutes les formes de communication"*, il est proposé d'énumérer le type de mesures ainsi visées.

Il y aurait ainsi trois types de mesures susceptibles d'être ordonnées:

---

31 Arrêt de la CJUE rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12

– la surveillance et le contrôle des télécommunications ainsi que de la correspondance postale,
– la sonorisation de certains lieux ou véhicules et
– la captation de données informatiques.

7.1. Champ d'application des mesures prévues aux articles 88-1 à 88-4

Les modifications introduites par les articles sous avis appellent les remarques suivantes:

– La sonorisation de lieux ou de véhicules (et surtout la sonorisation de lieux d'habitation) permet, certes, le contrôle des communications, mais elle va beaucoup plus loin que le simple contrôle des communications, alors qu'elle permet de surveiller tous les gestes et les habitudes de la vie quotidienne des personnes surveillées, (quand elles se lèvent et se couchent, quand elles cuisinent), la musique qu'elles écoutent ou les films qu'elles regardent, etc.
– De même la captation de données informatiques ne se limite pas aux communications: la captation peut concerner les documents que les personnes concernées rédigent sur leur ordinateur ou la saisie sur le clavier[32]. Elle permet aussi de contrôler les photos que les personnes surveillées affichent sur leur écran et enregistrent le cas échéant sur leur ordinateur, des images prises par la webcam, etc.

En ajoutant les sonorisations de lieux ou de véhicules et la captation de données informatiques aux mesures pouvant être prises dans le cadre des articles 88-1 à 88-4, on procède donc à un „saut en qualité" considérable des possibilités de surveillance. Aux mesures de contrôle proprement dites pourront aussi s'ajouter l'intrusion clandestine au domicile des personnes visées avant et après les opérations de contrôle, ainsi que l'introduction de logiciels sur les terminaux des personnes à surveiller.

De telles mesures vont donc largement au-delà de ce que permettent les articles 88-1 à 88-2 en leurs termes actuels. Comme il est précisé à juste titre dans le commentaire des articles, l'utilisation des articles 88-1 à 88-4 actuels à ces fins risquerait aussi de se heurter à l'exigence de précision de la jurisprudence de la Cour européenne des droits de l'homme.

Pour ce qui est du „saut en qualité" susmentionné, il faut également garder à l'esprit que les communications passées au domicile dans le cercle familial et privé peuvent revêtir un caractère plus intime que celles échangées par exemple par e-mail ou par courrier.

Vu le caractère extrêmement intrusif des mesures nouvellement introduites, il importe d'assortir les mesures de garanties suffisantes.

Ainsi, la Cour constitutionnelle allemande reconnaît dans ce contexte un noyau dur, un *„Kernbereich"* de la vie privée qui doit bénéficier d'une protection particulière. Cette notion de *„Kernbereich"* couvre par exemple les conversations tenues au domicile dans le cercle familial. Ainsi la cour a sanctionné les législations qui ne protègent pas à suffisance ce *„Kernbereich"* en matière de sonorisation[33] et de captation des données informatiques[34].

Suite à l'arrêt de la Cour constitutionnelle allemande du 3 mars 2004[35], la législation allemande applicable en matière de sonorisation[36] prévoit dorénavant une protection du *„Kernbereich"* à deux niveaux:

– Au niveau de la décision ordonnant la mesure: „*Die Maßnahme darf nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden* (…)".

---

32 Au moyen d'un „keylogger".

33 Arrêt concernant la législation applicable à la sonorisation ordonnée par les autorités judiciaires: Urteil vom 3. März 2004 – 1 BvR 2378/98. La question du *„Kernbereich"* est abordée aux points 157 à 268 de l'arrêt. Disponible sur „http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html".

34 Arrêt concernant la législation applicable à la captation de données informatiques opérée par le Landesverfassungsschutz de la Rhénanie-du-Nord-Westphalie: Urteil vom 27. Februar 2008 – 1 BvR 370/07. Voir points 270 à 287 de l'arrêt sur la question du *„Kernbereich"*. Disponible sur „http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html".

35 Arrêt 1 BvR 2378/98 précité

36 Strafprozeßordnung, § 100c Akustische Wohnraumüberwachung. Disponible sur „http://www.gesetze-im-internet.de/stpo/100c.html".

– Au niveau de l'exécution, qui doit le cas échéant être interrompue: *„Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Aufzeichnungen über solche Äußerungen sind unverzüglich zu löschen. Erkenntnisse über solche Äußerungen dürfen nicht verwertet werden. Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu dokumentieren."*.

Enfin, le caractère très intrusif des mesures pouvant être ordonnées sur base des articles 88-1 à 88-4 projetés est encore amplifié par le fait que le cercle des personnes visées est particulièrement large: Les mesures ne peuvent viser non seulement la personne suspecte, *„d'avoir commis l'infraction ou d'y avoir participé"*, mais également celle susceptible *„de recevoir* (le cas échéant contre son gré) *ou de transmettre des informations destinées à l'inculpé ou au suspect ou qui proviennent de lui"*.

Une limitation du cadre des personnes visées est nécessaire afin de garantir la prévisibilité de la mesure et d'arriver à un juste équilibre entre les droits fondamentaux des personnes et les intérêts des autorités répressives dans le cadre de la lutte contre le terrorisme.

7.2. Nécessité d'apporter des précisions quant aux données informatiques à capter

L'article 88-1 du projet de loi prévoit que le juge d'instruction puisse ordonner l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication qui permettent de capter des données informatiques. La Commission nationale estime qu'il est nécessaire que le Code d'instruction criminelle précise que l'ordonnance du juge d'instruction doit énoncer quel type de données informatiques peuvent être captées (p. ex. copies d'écran, contenus et métadonnées de communications électroniques, fichiers sur le disque dur, enregistrements audio, enregistrements de saisies au clavier, activation et captation de données de la webcam) afin de garantir une meilleure prévisibilité du texte[37]. La captation de données informatiques par les autorités judiciaires devrait donc se limiter aux données spécifiées dans l'ordonnance du juge d'instruction.

L'article 88-1 paragraphe (3) indique que les données informatiques captées peuvent inclure des données *„reçues et émises par des périphériques audiovisuels"* tels que les microphones ou les webcams intégrés au terminal infiltré. Or, ces périphériques peuvent enregistrer les conversations et les images d'autres personnes que du suspect, comme, par exemple, les membres de sa famille (ou toutes autres personnes présentes dans l'entourage du suspect) et permettent aussi de surveiller les locaux (ou les lieux) dans lesquels se trouve le terminal infiltré. La surveillance s'étend donc au-delà de la personne-même à surveiller, ce qui constitue une intrusion dans la vie privée de personnes en partie non-suspectes et est plus attentatoire à la vie privée que d'autres mesures de captation de données informatiques.

Une écoute (par le microphone de l'ordinateur) ou une vidéosurveillance (par la webcam de l'ordinateur) de l'intérieur d'un logement n'est pas toujours nécessaire et proportionnée et une autre forme de captation de données informatiques moins intrusive, comme p. ex. un contrôle des documents rédigés par la personne surveillée ou des images affichées sur son écran, peut suffire.

Dès lors, le texte de loi devrait également prévoir que l'ordonnance décidant de la mesure précise exactement et en détail quelles sont les opérations à effectuer. Il faut en tout cas éviter des ordonnances prescrivant simplement une „captation des données informatiques" sans donner davantage de détails.

7.3. Risques en matière de sécurité concernant la captation de données informatiques

La Commission nationale constate que les dispositifs techniques prévus pour capter des données informatiques risquent d'être exploités par des tiers (p. ex., services de renseignements étrangers[38],

---

37 Voir CNIL, *Délibération n° 2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement*, p. 7; Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). 27.2.2013, p. 97.

38 Sean Gallagher, *NSA secretly hijacked existing malware to spy on N. Korea*, Ars Technica, 19.1.2015. Disponible sur „http://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/".

cybercriminels[39]). Par exemple, si le dispositif contient des erreurs d'implémentation ou des backdoors, ces lacunes peuvent être exploitées par des tiers afin d'accéder aux données de la machine infiltrée. De plus, les entreprises qui développent les logiciels de surveillance sont souvent la cible d'attaquants et leurs clients, ainsi que le code source des logiciels, risquent d'être publiés sur Internet[40]. L'utilisation de ces dispositifs techniques crée des risques potentiels pour les citoyens.

La Commission nationale estime dès lors qu'il est indispensable de prendre les initiatives et mesures nécessaires pour garantir que a) le dispositif technique soit uniquement exploitable par les officiers de police judiciaire, qualifiés et habilités à cette fin, et b) que des procédures soient mises en place afin de désinstaller les logiciels pour lesquels des informations ont été révélées lors de cyberattaques.

De plus, la Commission nationale considère qu'il est primordial de soumettre les dispositifs techniques permettant la captation de données informatiques „à distance" via Internet à un contrôle de qualité à effectuer par des auditeurs externes et indépendants. Un tel contrôle de qualité permettrait de clarifier et de détecter, entre autres, si le dispositif peut être aisément exploité par des tiers, comme c'était le cas pour un dispositif développé par DigiTask et utilisé par le Bundeskriminalamt en Allemagne[41].

La Commission nationale constate qu'il n'est pas certain que les finalités poursuivies par la captation de données informatiques à l'aide de dispositifs techniques soient atteintes, ce qui jette des doutes sur l'efficacité de ce type de mesures. Il est, en effet, difficile de garantir qu'il n'existe pas de logiciels de sécurité (p. ex. logiciels open source ou développés par des entreprises) qui détectent ce type de logiciels de surveillance. Citons à ce sujet Eugene Kaspersky. CEO d'une entreprise qui vend des logiciels de sécurité: *„We detect all malware regardless its purpose&origin"*[42]. De plus, si la personne à surveiller se rend compte que sa machine a été infiltrée, il est fort probable qu'elle change de stratégie (et de moyens de communications).

Par ailleurs, la Commission nationale tient à souligner le risque élevé de cyberattaques contre les infrastructures, nécessitant une ouverture sur l'Internet et utilisées par les autorités répressives (p. ex. base de données centralisée) pour transmettre et stocker les données informatiques collectées à l'aide de dispositifs techniques installés sur les terminaux des personnes concernées. Par conséquent, afin de garantir la confidentialité des données captées, il est essentiel de mettre en place des mesures techniques et organisationnelles qui garantissent un haut niveau de sécurité.

La Commission nationale recommande partant de prévoir dans le texte de la loi l'obligation de chiffrer les données captées lors du transfert et lors du stockage, d'établir un système d'habilitations (droits d'accès, rôles, utilisateurs) afin de contrôler l'accès aux données captées et de tracer tous les événements qui ont trait à la captation de données informatiques à l'aide du dispositif technique (à partir de l'installation du dispositif jusqu'à la désinstallation du dispositif).

Ceci rejoindrait par ailleurs le texte de compromis du projet de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, qui dispose dans son article 24 que *„Member States shall ensure that logs are kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination or erasure ..."*[43].

---

39 Federal Trade Commission, *Spyware Workshop: Monitoring Software on your personal computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*, 7.3.2005.

40 Martin Steiger, *Sicherheitsesoterik statt Menschenrechte*, Digma 2015 – 4, p. 135.

41 Chaos Computer Club, *Analyse einer Regierungsmalware*, 8.10.2011. Disponible sur „http://www.ccc.de/system/uploads/76/original/staatstroianer-report23.pdf".

42 Mathew J. Schwartz, *FinFisher Mobile Spyware Tracking Political Activists*, Informaton Week, 31.8.2012. Disponible sur „http://www.darkreading.com/vulnerabilities-and-threats/finfisher-mobile/spyware-tracking-political-activists/dd-id/1106086?".

43 Article 24 du texte de compromis de la Directive relative à la protection des personnes physiques à égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, et à la libre circulation de ces données, 2012/0010 (COD), texte de compromis datant du 15 décembre 2015.

En outre, la Commission nationale s'interroge sur l'intégrité du système infiltré et des données informatiques captées. Il ne peut être exclu que l'installation du dispositif technique compromette l'intégrité du système et des données. De plus, si le dispositif technique installé sur le terminal d'une personne suspecte serait capable de manipuler (i.e., modifier, supprimer, ajouter) des données sur le terminal infiltré, il y aurait ainsi un risque que la police judiciaire collecterait des preuves falsifiées du terminal en question.

Par conséquent, la Commission nationale estime qu'il est nécessaire de mettre en place des mesures pour garantir l'intégrité des données informatiques collectées tant au niveau de la transmission de données qu'au niveau des données stockées sur le terminal. De telles mesures amélioreraient également la recevabilité et l'irréfutabilité de données captées en tant que preuves devant un juge.

Ainsi, le dispositif technique ne devrait permettre ni la manipulation de données sur le système infiltré, ni l'installation et l'activation de dispositifs techniques supplémentaires, distincts du dispositif technique de surveillance, ni d'ouvrir d'autres vulnérabilités dans le système infiltré[44]. La Commission nationale estime aussi nécessaire que les événements liés à l'installation du dispositif soient journalisés et que l'intégrité du système sur lequel le dispositif technique est installé soit préservée. De plus, le projet de loi devrait préciser les mesures de contrôle prises par le juge d'instruction lors de l'installation du dispositif de surveillance.

L'article 88-2 paragraphe (3) dispose que les mesures de surveillance *„doivent être levées dès qu'elles ne sont plus nécessaires"*. Or, comment peut-on garantir le retrait du dispositif technique d'un terminal infiltré? Quelles procédures techniques et organisationnelles seront appliquées pour désactiver et désinstaller le dispositif? S'agit-il d'une désinstallation automatique qui aura lieu après un temps défini à compter de la date de l'ordonnance du juge d'instruction?

Il est nécessaire de préciser les modalités exactes de la désinstallation du dispositif technique de terminaux infiltrés et les modalités de suppression des données informatiques captées de personnes qui ont été surveillées à tort ou qui se révèlent non suspectes au cours de la surveillance.

Lorsque le dispositif technique a modifié le système du terminal infiltré, le dommage subi par la personne surveillée, mais surtout l'origine du dommage, seront difficile à prouver en cas de recours contre l'Etat.

La Commission nationale s'interroge, en conséquence, sur la proportionnalité des mesures de surveillance envisagées par rapport aux buts recherchées et aux résultats escomptés et recommande de prévoir des garanties supplémentaires afin de mitiger les risques liés à ce traitement de données et de limiter l'intrusion dans la sphère privée des personnes concernées et de leur environnement.

7.4. Secret professionnel et protection des sources du journaliste

Le projet de loi prévoit la protection des personnes liées par le secret professionnel. Pourtant, la protection n'est pas absolue, puisqu'elle ne joue que si les individus détenteurs du secret professionnel ne sont pas *„suspects d'avoir elles-mêmes commis l'infraction ou d'y avoir participé"*.

7.4.1. *Protection prévue par les articles*

Les articles 88-2 paragraphe (5) et 88-4 paragraphe (3) reprennent les dispositions déjà contenues dans les articles 88-1 et 88-2 du Code d'instruction criminelle:

– *„Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne peuvent être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction."* (article 88-2 paragraphe (5) projeté)
– *„Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne*

---

44 Voir aussi Chaos Computer Club, *Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern*, 7.7.2015, p. 5; *Nationalratskommission befürwortet Staatstrojaner, TagesAnzeiger, 17.4.2015. Disponsible sur*

„http://www.tagesanzeiger.ch/schweiz/standard/Nationalratskommission-befuerwortet-Staatstrojaner/story/11016889".

peuvent être utilisées. Leur enregistrement et leur transcription sont immédiatement détruits par le juge d'instruction." (article 88-4 paragraphe (3) projeté)

7.4.2. *Protection des sources du journaliste*

Seules les personnes liées par le secret professionnel au sens de l'article 458 du Code pénal sont couvertes par cette disposition.

En revanche, les journalistes, qui ne sont pas liés par un secret professionnel, ne sont donc pas protégés par les dispositions susmentionnées. En effet, la protection des sources du journaliste n'est pas à assimiler à un secret professionnel[45].

Comme en matière d'accès aux données de trafic de communications[46], on peut se demander si la protection prévue par la loi du 8 juin 2004 sur la liberté d'expression dans les médias est suffisante[47].

Ne faudrait-il pas prévoir une protection expresse des journalistes dans les articles 88-1 à 88-4 projetés du Code d'instruction criminelle à l'instar notamment de la législation française qui a servi d'exemple pour les modifications projetées des articles 88-1 et suivants?

Le Code de procédure pénale français prévoit en effet une protection expresse des journalistes, aussi bien en matière de sonorisation[48], qu'en matière de captation des données informatiques[49]. Y sont protégés *„les locaux d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne, d'une agence de presse, dans les véhicules professionnels de ces entreprises ou agences ou au domicile d'un journaliste lorsque les investigations sont liées à son activité professionnelle"*.

7.4.3. *Etendue de la protection et incidence de l'introduction des mesures de sonorisations de lieux ou véhicules et de captation de données informatiques*

Alors que les articles 88-1 et 88-2 s'appliquent aujourd'hui aux communications électroniques et postales, ce sont *les communications* avec des personnes liées par le secret professionnel qui sont protégées. Vu l'introduction des mesures de sonorisation de lieux ou véhicules et de captation de données informatiques, il se pose la question de savoir s'il ne faudrait pas désormais protéger aussi les lieux où travaillent les personnes protégées (contre la sonorisation) et les *lieux* où se trouvent des systèmes informatiques, voire les systèmes informatiques eux-mêmes utilisés par les personnes protégées (contre la captation des données informatiques).

L'article 706-96 alinéa 3 du code de procédure pénale français sur les sonorisations est formulé de la manière suivante:

„La mise en place du dispositif technique mentionné au premier alinéa ne peut concerner les lieux visés aux articles 56-1, 56-2 et 56-3 ni être mise en oeuvre dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7."

En matière de captation des données informatiques, la formulation est la suivante:

„La mise en place du dispositif technique mentionné à l'article 706-102-1 ne peut concerner les systèmes automatisés de traitement des données se trouvant dans les lieux visés aux articles 56-1,

---

45 *„La protection des sources journalistiques ne doit pas être confondue avec le secret professionnel. Celui-ci est une obligation alors que celle-là est une protection. Dans le premier cas, il est interdit de dire; dans le second, il est permis de ne pas dire."* Loïc DENIS, *La protection des sources journalistiques*, dans *LES CAHIERS DU JOURNALISME NO13 – PRINTEMPS 2004*. Disponible sur

„wvvw.cahiersdujournalisme.net/cdj/pdf/13/18_Denis.pdf".

46 Point 2.2. du présent avis

47 Pour un cas de figure postérieur à la loi du 8 juin 2004 (non en matière de contrôle des communications mais en matière de perquisition): cf. l'arrêt précité de la Cour européenne des droits de l'homme (Cinquième section), affaire Saint-Paul Luxembourg S.A. c. Luxembourg, requête n° 2641910 du 18 avril 2013.

48 Article 706-96 du Code de procédure pénale français renvoyant à la liste des lieux protégés énumérés à l'article 56-2.

49 Article 706-102-5 du Code de procédure pénale français renvoyant à la liste des lieux protégés énumérés à l'article 56-2.

56-2 et 56-3 ni être réalisée dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7.“[50].

Au vu des considérations ci-avant, la Commission nationale recommande fortement d'étendre et d'adapter en ce sens la protection dans la législation luxembourgeoise.

7.5. Protection physique des données obtenues

Les données obtenues suite à la captation informatique et, dans une moindre mesure, les enregistrements sonores, sont facilement susceptibles de faire l'objet de manipulations. Dès lors, il faut les protéger de manière adéquate.

Des mesures protectrices efficaces représentent non seulement une garantie indispensable pour le justiciable, mais protègent aussi l'institution judiciaire contre des contestations injustifiées et allégations de manipulations.

Elles s'imposeront en tout état de cause en vertu de l'article 27 du projet de Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données[51].

L'article 88-4 paragraphe 2 projeté[52] prévoit ce qui suit:

„Les télécommunications enregistrées et les correspondances, ainsi que les données ou renseignements obtenus par d'autres moyens techniques de surveillance et de contrôle sur la base de l'article 88-1 sont remis sous scellés et contre récépissé au juge d'instruction qui dresse procès-verbal de leur remise. Il fait copier les correspondances pouvant servir à conviction ou à décharge et verse ces copies, les enregistrements ainsi que tous autres données et renseignements reçus au dossier […].“

L'article ne précise pas par qui, quand et comment les enregistrements sont mis sous scellé.

L'article dispose que les correspondances font l'objet de copies qui sont jointes au dossier. En revanche, à lire l'article, les enregistrements sonores et informatiques seraient joints au dossier sous leur forme „originale“ (sous laquelle ils ont été remis au juge d'instruction).

Il semble évident que les enregistrements doivent être maniés et consultés au cours de l'instruction, si ce n'est que pour faire l'objet de copies, à moins qu'ils aient fait l'objet d'un procès-verbal exhaustif avant la mise sous scellé, ce qui paraît encore imaginable pour des enregistrements sonores, mais l'est moins pour certains enregistrements issues d'une captation de données informatiques (et en toute état de cause, cette hypothèse devrait être précisée dans le texte).

Il est donc fort probable que les scellés doivent être ouverts. Cependant, rien ne précise que les enregistrements doivent, de nouveau, être remis sous scellé après ouverture.

Or, entre ce moment de l'ouverture des scellés et l'intervention d'un jugement définitif, des années peuvent s'écouler et les données doivent également être soumises protégées pendant cette durée.

Enfin, le sort des enregistrements obtenus en cas d'expertise ordonnée sur base des articles 87 ou 88 du Code d'instruction criminelle n'est pas clair non plus.

L'article 163 du Code de procédure pénale français dispose à ce sujet ce qui suit:

„Pour l'application de leur mission, les experts sont habilités à procéder à l'ouverture ou à la réouverture des scellés et à confectionner de nouveaux scellés après avoir, le cas échéant, procédé au reconditionnement des objets qu'ils étaient chargés d'examiner; dans ce cas, ils en font mention dans leur rapport, après avoir, s'il y a lieu, dressé inventaire des scellés; …“

La Commission nationale recommande de compléter les dispositions relatives à la mise sous scellé afin de donner des réponses aux questions et problèmes formulés ci-dessus.

---

50 Article 706-102-5 alinéa 3 du Code de procédure pénale français.

51

52 Artice 88-2 alinéa 3 actuel.

7.6. Information des personnes concernées

Le droit à l'information des personnes concernées est un gage de transparence face à des investigations qui constituent une ingérence grave dans la vie privée de ces personnes.

L'information des personnes concernées est également nécessaire afin que les voies de recours existant en théorie puissent être exercées en pratique.

7.6.1. *Personnes visées*

L'information est prévue au bénéfice de *„la personne dont les communications ont été surveillées"*. Pour la Commission nationale, il n'est pas clair s'il s'agit uniquement de la personne suspectée ou aussi d'autres personnes concernées comme par exemple des membres de famille cohabitant dans le même logement (faisant l'objet d'une sonorisation) ou utilisant le même ordinateur (faisant l'objet d'une captation de données informatiques) que la personne suspectée, dans l'hypothèse où ces autres personnes concernées sont connues.

Pour ce qui est plus particulièrement de la sonorisation de lieux privés, la Cour constitutionnelle allemande a d'ailleurs décidé ce qui suit:

„Die Benachrichtigungspflicht dient der Gewährleistung effektiven Schutzes der hier betroffenen Grundrechte. Demzufolge sind all diejenigen von der heimlichen Maßnahme zu unterrichten, in deren Grundrechte durch sie eingegriffen worden ist und denen somit Rechtsschutzmöglichkeiten und Anhörungsrechte offen stehen müssen. Zielperson einer akustischen Wohnraumüberwachung ist zwar allein der Beschuldigte. Der Grundrechtseingriff einer akustischen Wohnraumüberwachung bleibt aber nicht auf diesen begrenzt.

Als Beteiligte im Sinne des § 101 Abs. 1 StPO sind daher neben dem Beschuldigten die lnhaber und Bewohner einer Wohnung zu benachrichtigen, in denen Abhörmaßnahmen durchgeführt worden sind.

Eine Benachrichtigungspflicht besteht grundsätzlich auch gegenüber solchen Personen, die sich als Gast oder sonst zufäIlig in einer überwachten Wohnung aufgehalten haben und die in ihrem durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützten Recht am gesprochenen Wort und in ihrem informationellen Selbstbestimmungsrecht betroffen sind."[53]

La Commission nationale estime dès lors nécessaire de préciser les destinataires de l'information.

7.6.2. *Délais et exceptions*

L'information a lieu *„au cours même de l'instruction et en tout cas au plus tard dans les douze mois qui suivent la cessation de la prédite mesure."*

Cependant, dans le cadre des infractions pour lesquelles le juge d'instruction pourrait avoir recours aux mesures de sonorisation de lieux ou véhicules et de captation de données informatiques, la loi prévoit une exception à ce délai de 12 mois. Une telle exception, qui permettrait aux autorités de retarder sans limitation l'information, risque de priver la personne de son droit à l'information.

D'ailleurs, en matière de sonorisation, la Cour constitutionnelle allemande a décidé ce qui suit:

„Um sicherzustellen, dass die Zurückstellung [der Benachrichtigung] *auch im weiteren Verlauf auf das unbedingt Erforderliche begrenzt bleibt, bedarf es in Zeitabständen einer wiederkehrenden gerichtlichen Überprüfung"*[54].

La Commission nationale fait siennes les réflexions de la Cour constitutionnelle allemande pour recommander de permettre un retardement de l'information que sur décision explicite et pour une période limitée dans le temps, le cas échéant renouvelable, après un contrôle juridictionnel.

---

53 Points 294 à 296 de l'arrêt précité du 3 mars 2004.

54 Point 306 de l'arrêt précité du 3 mars 2004.

7.7. Voies de recours

Il est prévu de supprimer le recours de l'opposition prévu initialement pour le contrôle des communications. Selon le commentaire des articles, il existerait des recours adéquats (y compris pour des tiers) en la forme du recours en nullité prévu par l'article 126 du Code d'instruction criminelle.

A défaut de jurisprudence publiée en matière de contrôle des communications effectué sur base des articles 88-1 et 88-2 du Code d'instruction criminelle, il est difficile d'apprécier l'efficacité des voies de recours.

On constate cependant que la plupart des conditions des articles 88-1 à 88-4 projetés du Code d'instruction criminelle ne sont pas prescrites à peine de nullité. Tel est notamment le cas pour la nécessité d'une infraction ayant trait au terrorisme pour les mesures de sonorisation de lieux ou véhicules et de captation de données informatiques, la nécessaire inopérance des moyens ordinaires d'investigation, l'exigence d'une décision spécialement motivée, la limitation dans le temps de la mesure, l'approbation par le président de la chambre du conseil de la prolongation de la mesure, ainsi que de l'introduction dans un lieu privé et de l'installation par Internet d'un logiciel d'espionnage, l'interdiction d'appliquer la mesure à l'inculpé et la protection des personnes titulaires d'un secret professionnel.

Pour la Commission nationale, toutes ces conditions devraient être prescrites à peine de nullité afin de garantir au mieux possible leur respect et d'assurer leur sanction en cas de non-respect eu égard à l'intrusion grave dans la vie privée.

Enfin, les personnes concernées, et les tiers en particulier ne peuvent vraiment faire usage des voies de recours que s'ils ont connaissance des mesures ordonnées. A ce sujet, il est renvoyé aux développements exposés ci-dessus relatifs au droit à l'information des personnes surveillées.

7.8. Conclusion

La Commission nationale s'interroge sur la proportionnalité des mesures de surveillance envisagées par rapport aux buts recherchées et aux résultats escomptés et recommande de prévoir des garanties supplémentaires afin de garantir la prévisibilité de la mesure et d'arriver à un juste équilibre entre les droits fondamentaux des personnes et les intérêts des autorités répressives dans le cadre de la lutte contre le terrorisme et de mitiger les risques liés à ce traitement de données, ainsi que de limiter l'intrusion dans la sphère privée des personnes concernées et de leur environnement.

La Commission nationale recommande dès lors de compléter les dispositions des articles sous avis, afin d'apporter des réponses aux problématiques soulevées ci-dessus.

*

8. ARTICLE 41 DE LA LOI MODIFIEE DU 2 AOUT 2002 RELATIVE A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Le présent article vise à réintroduire une disposition abrogée en 2011 en raison essentiellement de difficultés techniques. Selon l'exposé des motifs, l'instrument conçu par la loi de 2002 est, à supposer opérationnel, d'une efficacité indiscutable. Il évite de devoir procéder, comme en l'état actuel du droit, à des perquisitions auprès des opérateurs pour obtenir les informations en question, et après mise en vigueur de l'article 48-27 tel que proposé, de devoir adresser des réquisitions aux opérateurs. L'instrument permet beaucoup plus simplement un accès direct et à distance par voie de communication électronique aux informations en question.

8.1. Insertion dans la loi de 2002

Le projet de loi sous avis prévoit d'insérer les dispositions relatives au nouveau traitement de données à effectuer notamment par l'Institut Luxembourgeois de Régulation (ILR) dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Cette loi a pour objet de transposer la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Or, la directive 95/46/CE est sur le point d'être remplacée par le nouveau règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[55].

Le fait que le règlement soit directement applicable, risque d'avoir comme conséquence que la loi modifiée du 2 août 2002 sous sa forme actuelle disparaisse prochainement[56].

8.2. Manque de précisions concernant les données traitées

L'élément clé de ce traitement de données, à savoir les données traitées, n'est pas déterminé dans le texte et serait fixé dans un règlement grand-ducal. Ainsi, la loi ne s'exprime pas clairement sur la nature des données visées.

Or, l'article 11 paragraphe (3) de la Constitution dispose ce qui suit: *„L'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi"*. Selon la jurisprudence de la Cour constitutionnelle, *„dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc"*[57]. L'article 41 projeté ne saurait guère satisfaire à cette exigence.

Par ailleurs, les termes de l'article ne permettent pas d'exclure avec certitude que des données relatives au trafic des communications effectuées ne soient visées[58].

La Commission nationale estime nécessaire que la loi énumère en détail les données d'identification visées, à l'instar de l'article 7 paragraphe (5) ou des articles 5 et 9 (où un règlement grand-ducal prévoit le détail des données) de la loi du 30 mai 2005 et de façon générale, agencer la terminologie employée sur celle de l'article 48-27.

8.3. Nature de l'accès

L'article 41 est une des façons d'accéder aux données prévues par l'article 48-27 et l'accès prévu par le présent texte est subordonné aux conditions dudit article. Alors que l'accès est direct et à distance par voie de communication électronique, il procure selon les auteurs du projet de loi un gain d'efficacité spectaculaire.

La Commission nationale constate que l'accès est soumis aux conditions de l'article 48-27. Les données ne peuvent être accédées que dans des cas spécifiques, pour des recherches déterminées et dans le respect de procédures strictes. Ces garanties indispensables sont toutefois menacées par le paragraphe (4) dudit article en ce qu'il dispose que *„La procédure est entièrement automatisée suite à l'autorisation de la Commission nationale."*

En effet, une procédure entièrement automatisée laisse peu de place pour le respect de procédures, à moins que ce ne soit que le volet de la transmission des données des opérateurs et des fournisseurs vers l'ILR qui soit visé. La Commission nationale recommande de préciser ce point.

8.4. Durée de conservation

La loi ne précise rien quant à la durée de conservation des données auprès de l'ILR.

Il n'est pas clair si lors de la mise à jour des données qui doit avoir lieu une fois par jour au moins, les données anciennes sont effacées de manière automatique, ou si les données sont empilées jusqu'à

---

55 A ce règlement s'ajoutera, en matière répressive, la directive précitée relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

56 Même si une loi nationale devra régler un certain nombre de questions institutionnelles et procédurales relatives au nouveau règlement.

57 Arrêt 117 de la Cour constitutionnelle.

58 La Commission nationale se demande si les *„données concernant l'identité* (…) *des utilisateurs"* incluent des données précises relatives à l'identité de la personne ayant passé telle ou telle communication donnée.

l'infini, ou bien si elles sont effacées après un certain délai. Ce sont des questions auxquelles la loi devrait répondre afin de répondre aux exigences de précision et de prévisibilité de jurisprudence de la Cour européenne des droits de l'homme en matière d'ingérence au droit au respect de la vie privée.

Rappelons aussi que, dans son arrêt rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, la Cour de justice de l'Union européenne a fustigé le fait que la directive 2006/24/CE laisse, pour ce qui est de la durée de conservation, une marge s'étendant de 6 mois à 2 ans sans donner davantage de précisions[59]. Or, en l'espèce, aucune durée de conservation du tout n'est fixée.

La durée de conservation ne doit en aucun cas être disproportionnée par rapport aux finalités du traitement.

8.5. Nécessité et proportionnalité du traitement de données envisagé

Le présent projet tend à mettre en place un système qui permet d'accéder aux données concernant l'utilisation de moyens de communication de pratiquement tous les citoyens habitant le pays, accès qui peut être effectué non seulement en cas de suspicion de terrorisme, mais pour tout crime ou délit.

Si le système est indispensable pour assurer la lutte contre la criminalité, celle-ci devrait être moins effective dans les pays ne disposant pas d'un tel système, ce qui n'est pas avéré.

Par ailleurs, des voies alternatives moins attentatoires à la vie privée comme une accélération des procédures sans création d'une nouvelle banque de données, devraient être explorées avant la mise en place d'un tel système.

Pour le surplus, la Commission nationale renvoie à ses développements au point 5.2.

8.6. Le cas particulier des services de secours

L'article 41 réintroduit également un droit d'accès pour la Centrale des secours d'urgence et la Centrale du service d'incendie et de sauvetage de la Ville de Luxembourg aux mêmes conditions et modalités que les autres autorités visées par cet article.

L'accès à ces données par les services de secours constitue une finalité toute à fait différente de celle poursuivie par les autorités répressives. Ni le projet de loi, ni l'exposé des motifs ou le commentaire des articles fournissent des précisions sur le motif des services de secours qui doit certainement être recherché dans son propre cadre législatif, mais qui vise peu probablement la prévention, la recherche, la constatation ou la poursuite d'infractions. La Commission nationale considère que pour le cas où un recours à un tel mécanisme devrait être nécessaire, l'accès par les services de secours ne devrait pas figurer parmi les dispositions de l'article 41 de la loi du 2 août 2002 réintroduit dans la loi dans un but de renforcer les moyens de lutte contre le terrorisme, mais plutôt dans une loi spéciale réglementant les pouvoirs des services de secours.

Par ailleurs, la Commission nationale estime qu'en présence de l'article 4 paragraphe (3) lettre (c) et surtout de l'article 7 paragraphe (5) lettre (a) de la loi du 30 mai 2005 précitée, les services de secours disposent des accès aux données nécessaires à l'atteinte de leurs finalités et qu'il n'y a pas besoin de prévoir des mécanismes supplémentaires.

En effet, l'article 7 „Identification de la ligne appelante et la ligne connectée" dispose en son paragraphe (5) *„(a) Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminées par l'Institut luxembourgeois de régulation transmet („push") pour chaque appel à destination d'un de ces numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation."*

Le point (c) rajoute que *„Pour les appels effectués à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminées par l'Institut, l'identification de la ligne appelante „et les données de localisation de l'appelant" sont toujours présentées même lorsque l'appelant les a empêchés."*

L'article 4 paragraphe (3) prévoit une exception à la confidentialité des communications en faveur du numéro d'urgence unique européen 112 et des numéros d'urgence déterminées par l'Institut de

---

59 Considérants 63 et 64.

Régulation Luxembourgeois en vertu de laquelle les communications peuvent être enregistrées à partir de ces numéros.

Notons que le Règlement 14/182/ILR du 26 août 2014 relatif à la détermination de numéros d'urgence au sens de la loi du 30 mai 2005, considère en plus du numéro d'appel d'urgence unique européen „112", comme numéros d'urgence au sens de l'article 4 paragraphe (3) et de l'article 7 paragraphe (5) lettres (a) et (c) le numéro „113" de la Police Grand-Ducale et le numéro „44 22 44" du Service d'Incendie et de sauvetage de la Ville de Luxembourg.

Les numéros des six Centres d'Intervention Principaux de la Police Grand-Ducale sont considérés comme numéros d'urgence au sens de l'article 4 paragraphe (3) lettre (c) de la loi de 2005.

Pour le cas où le législateur devrait néanmoins décider de maintenir l'accès des données par les services de secours en vertu de l'article 41, la Commission nationale s'étonne sur les conditions et modalités dans lesquels cet accès devrait s'effectuer. Vu le libellé actuel du texte en projet et en l'absence de précisions à ce sujet, la Commission nationale doit supposer qu'un accord du moins oral du juge d'instruction ou du Procureur d'Etat doit précéder toute consultation, qui elle doit être spécifique. Ceci n'est certainement pas la réelle volonté des auteurs du projet de loi, car adopter les mêmes conditions et modalités pour les besoins des services de secours risquerait d'entraver leur bon fonctionnement. Quoi qu'il en soit retenu, il est évident que l'accès par les services de secours doit être proportionné à leur finalité et entouré des garanties appropriées nécessaires à la protection des droits fondamentaux des individus concernés.

8.7. Absence de règles de sécurité

La loi ne prévoit pas de règles de sécurité particulières afin de protéger au mieux le nouveau traitement de données.

Certes, les articles 22 et 23 de la loi modifiée du 2 août 2002 sont en principe applicables. Cependant, ces articles laissent une marge de manoeuvre beaucoup trop grande et ne sont pas suffisantes pour un traitement d'une telle envergure[60].

Rappelons qu'en matière de rétention de données de communications électroniques, la Cour de justice de l'Union européenne a, dans son arrêt précité du 8 avril 2014, déclaré invalide la directive 2006/24/CE notamment parce que celle-ci *„ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles"*[61]

En l'espèce, il faudrait assurer, pour ce qui est du traitement en général et des procédures automatisées de transmission en particulier, un niveau de sécurité particulièrement élevé.

Par ailleurs, il faudrait prévoir dans la loi une conservation, dans un log, des données relatives à l'identité des personnes accédant aux données, au moment et au motif de la consultation (avec, le cas échéant, la référence de la décision du magistrat prise en vertu de par l'article 48-27 projeté du Code d'instruction criminelle), à l'image de ce qui se fait pour les accès des officiers de police judiciaire ou des magistrats aux banques de données d'administrations publiques en vertu de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police respectivement de l'article 48-24 du Code d'instruction criminelle.

L'absence de règles de sécurité ne saurait être réparée par l'exigence de l'autorisation à délivrer par la Commission nationale. En effet, une procédure d'autorisation devrait avoir comme objectif plutôt de faire veiller au respect de la loi, que de parer aux carences de celle-ci.

---

60 A titre d'exemple, en Allemagne, la loi nationale transposant la directive 2006/24/CE a été déclarée anticonstitutionnelle notamment en raison de l'absence de règles de sécurité spécifiques adaptées à l'ampleur du traitement de données, les règles générales de sécurité applicables en matière de protection des données étant insuffisantes: *„Das Fehlen hinreichender Sicherheitsstandards im Telekommunikationsgesetz kann auch § 9 BDSG in Verbindung mit der zugehörigen Anlage nicht ausgleichen. Unbeschadet ihrer zum Teil abstrakt hohen Standards bleibt diese Norm, die ohnehin nur subsidiär anwendbar ist (vgl. Fetzer, in: Arndt/Fetzer/Scherer, TKG, 2008, vor § 91 Rn. 10; Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 91 Rn. 15), zu allgemein, um in hinreichend spezifischer und verlässlicher Weise die besonders hohen Sicherheitsstandards bezüglich der nach 113a TKG zu speichernden Daten sicherzustellen."* Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, point 274 de l'arrêt. Le § 9 BDSG y mentionné et son „Anlage" correspondent aux articles 22 paragraphe (1) et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

61 Considérant 67 de l'arrêt.

8.8. La procédure d'autorisation

8.8.1. *Objet de l'autorisation*

A la différence de la plupart des autorisations que la Commission nationale délivre habituellement et qui couvrent tous les aspects d'un traitement de données à caractère personnel, l'autorisation à délivrer en l'espèce est limitée à *„la procédure"* (ou les modalités du caractère automatisé de cette procédure) et exclut bon nombre d'aspects:

– L'existence même du système est prévue par l'article 41 projeté de la loi modifiée du 2 août 2002.
– Les destinataires sont fixés par l'article 41 projeté ainsi que par l'article 48-27 projeté du Code d'instruction criminelle.
– Les données traitées seront fixées par règlement grand-ducal.
– Le *„format et les modalités de mises à disposition des données"* seront également fixées par règlement grand-ducal.

Des questions relatives au champ d'application de la procédure d'autorisation subsistent:

– Est-ce que *„la procédure"* à autoriser en vertu du paragraphe (4) de l'article 41 projeté est uniquement celle relative à l'accès aux données par les destinataires finaux, accès évoqué dans les paragraphes (3) et (4) *in fine*? Dans l'affirmative, la transmission des données de l'ILR vers les destinataires finaux (magistrats, services de secours) ferait, certes, partie du champ d'application de la procédure d'autorisation. En revanche, la transmission (probablement plus massive) de données des fournisseurs de service et opérateurs vers l'ILR en serait exclue.
– Ou bien *„la procédure"* couvre-t-elle aussi la transmission de données des fournisseurs de service et opérateurs vers l'ILR qui est réglée par le paragraphe (2) de l'article 41. Dans cette hypothèse, il se poserait la question de la limite entre *„le format et les modalités de mises à disposition des données"* à fixer par règlement grand-ducal et *„la procédure"* à autoriser par la Commission nationale.
– Est-ce que les questions relatives au stockage des données indépendantes de la question de la transmission font partie de *„la procédure"*?

La Commission nationale se demande aussi s'il n'y a pas un risque qu'en l'espèce, un traitement se trouve en quelque sorte labellisé *„autorisé par la Commission nationale"*, alors que l'emprise réelle de la Commission nationale dans le cadre de cette procédure d'autorisation est très limitée.

8.8.2. *En cas de refus*

Que se passerait-t-il en cas de refus par la CNPD? L'autorisation ne portant pas sur l'existence même du système dans son ensemble, mais uniquement sur la procédure d'accès automatisée, le système devrait être mis en place sans l'accès automatisé. Or, cela n'aurait guère de sens, étant donné que la raison d'être affichée du nouveau système est justement sa rapidité obtenue grâce à l'accès automatisé.

8.9. Conclusion

Pour la Commission nationale, les modalités de mise en oeuvre de ce nouveau traitement de données ne sont pas suffisamment claires. Dès lors, elle ne peut se prononcer en pleine connaissance de cause.

Si néanmoins le principe de l'introduction d'un tel traitement de données devait être retenu, celui-ci devrait répondre aux questions et exigences formulées ci-dessus.

Ainsi décidé à Esch-sur-Alzette en date du 12 février 2016.

La Commission nationale pour la protection des données

Tine A. LARSEN	Thierry LALLEMANG	Georges WANTZ
Présidente	*Membre effectif*	*Membre effectif*