Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7424 portant création d'une plateforme commune de transmission électronique sécurisée et modification : 1. du code de procédure pénale, 2. de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

Délibération n° 40/2019 du 5 juin 2019

Conformément à l'article 57, paragraphe 1, lettre c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (ci-après : « le RGPD »), chaque autorité de contrôle a, dans le cadre du champ d'application du RGPD, pour mission de conseiller « *conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ». L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après : « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Conformément à l'article 8, point 3°, de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD a, dans le cadre de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, notamment pour mission de « *conseille[r] la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données personnelles* »[1].

Par courrier du 15 mars 2019, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n°7424 portant création d'une plateforme commune de transmission électronique sécurisée et modification : 1. du code de procédure pénale, 2. de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat (ci-après : « le projet de loi »).

Il résulte de l'exposé des motifs que le projet de loi vise à mettre en place une plateforme commune et unique de transmission électronique sécurisée servant aux autorités judiciaires ainsi qu'au Service de renseignement de l'Etat (ci-après : « la plateforme »). Selon les auteurs du projet de loi, la plateforme offre une protection accrue des données personnelles des personnes faisant l'objet de mesures de repérage, de surveillance ou de contrôle.

[1] En ce qui concerne les champs d'application respectifs du RGPD et de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, voir notamment : D. Jeitz et T.A. Larsen, « Le futur régime de la protection des données dans les secteurs judiciaire et policier », Journal des tribunaux Luxembourg, n°54, 5 décembre 2017, pages 168-175

La Commission nationale constate toutefois que le projet de loi reste muet sur les mesures techniques et organisationnelles à mettre en place pour garantir un niveau de sécurité adapté au regard de la sensibilité des données transmises via la plateforme, d'autant plus que le titre du projet de loi annonce la création d'une plateforme électronique « sécurisée ». De plus, elle regrette que le projet de règlement grand-ducal qui est censé définir le format et les modalités d'exécution suivant lesquelles les données collectées sont à transmettre respectivement aux autorités judiciaires et au Service de renseignement de l'Etat n'a pas été annexé au projet de loi.

La CNPD souhaite formuler des commentaires et réflexions sur le projet de loi, en suivant pour cela l'ordre de rédaction du texte.

I. Champ d'application

L'article 1 du projet de loi définit le champ d'application du texte sous examen en renvoyant à plusieurs articles du Code de procédure pénale ainsi qu'à l'article 7 de la loi modifiée du 5 juillet 2016 portant organisation du Service de renseignement de l'Etat (ci-après : « la loi du 5 juillet 2016 »).

Avant de se pencher sur le moyen technique permettant aux autorités judiciaires et au Service de renseignement de l'Etat d'accéder aux données conservées par les fournisseurs de réseau de communication public ou de services de communications électroniques, la Commission nationale souhaite formuler des observations sur le principe même de la conservation et de l'accès aux données de trafic et de localisation relatives aux communications électroniques.

A. L'article 43-1 du Code de procédure pénale

En cas de disparition d'une personne, l'article 43-1, alinéa 1, du Code de procédure pénale permet aux officiers de police judiciaire de procéder, sur instructions du procureur d'Etat, aux actes prévus aux articles 31 à 41 du Code de procédure pénale, c'est-à-dire aux actes prévus en cas de flagrant crime ou délit, aux fins de découvrir la personne disparue.

Or, contrairement à ce qui est indiqué à l'article 3, paragraphe 1, point 1°, du projet de loi, ni l'article 43-1 ni les articles 31 à 41 du Code de procédure pénale ne semblent prévoir de « procédure de localisation ».

A toutes fins utiles, la Commission nationale se permet de renvoyer à un arrêt de la Cour d'appel du 26 février 2008 selon lequel « *le repérage est depuis l'entrée en vigueur de l'article 67-1 réservé à la compétence exclusive du juge d'instruction* » de sorte que l'article 67-1 « *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 (actuellement Code de procédure pénale)]* »[2].

Par ailleurs, la loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications

[2] Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V

électroniques et de l'article 67-1 du Code d'instruction criminelle (ci-après : « la loi du 24 juillet 2010 ») a modifié, suite à la recommandation formulée par la Commission nationale dans son avis du 26 avril 2010[3], le paragraphe 2 des articles 5 et 9 de la loi modifiée du 30 mai 2005 « *pour en assurer la cohérence avec l'article 67-1 du Code d'instruction criminelle aux termes duquel le repérage des communications n'est possible que s'il est ordonné par le juge d'instruction* »[4].

La CNPD se pose dès lors la question de savoir dans quelle mesure le projet de loi est susceptible de s'appliquer aux mesures ordonnées sur base de l'article 43-1 du Code de procédure pénale, respectivement quelle est précisément la *« procédure de localisation prévue par l'article 43-1 du Code de procédure pénale »*.

B. Les articles 67-1 et 88-1 du Code de procédure pénale

L'article 67-1 du Code de procédure pénale autorise le juge d'instruction de faire procéder au repérage des données d'appel de moyens de télécommunications à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés ainsi qu'à la localisation de l'origine ou de la destination de télécommunications.

L'article 88-1 du Code de procédure pénale, quant à lui, prévoit notamment la possibilité pour le juge d'instruction d'ordonner la surveillance et le contrôle des télécommunications ainsi que de la correspondance postale.

Dans le cadre des mesures prévues aux articles 67-1 et 88-1 du Code de procédure pénale, les autorités judiciaires peuvent être amenées à accéder aux données de trafic ou de localisation que les fournisseurs de service ou les opérateurs sont obligées de conserver en vertu des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (ci-après : « la loi modifiée du 30 mai 2005 »).

L'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans notre législation nationale par la loi modifiée du 30 mai 2005, cela sur base de l'article 15, paragraphe 1, de 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 (ci-après : « la directive 2002/58/CE »).

L'article 15, paragraphe 1, de la directive 2002/58/CE permet une telle mesure lorsqu'une telle limitation des principes prévus aux articles 5,6,8 et 9 constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique notamment pour sauvegarder la sûreté de l'Etat ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Par la suite, la loi du 24 juillet 2010 a transposé la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le

[3] Délibération n°85/2010 du 26 avril 2010, point I. B. 2. : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2010/retention-donnes/avis_CNPD_projet_loi_6113.pdf
[4] Projet de loi n°6113/8, p. 2

cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (ci-après : « la directive 2006/24/CE ») en modifiant la loi modifiée du 30 mai 2005.

Or, par arrêt du 8 avril 2014, la Cour de justice de l'Union européenne (ci-après : « la CJUE ») a déclaré invalide la directive 2006/24/CE en ce que le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7 (respect de la vie privée et familiale), 8 (protection des données à caractère personnel) et 52, paragraphe 1 (portée et interprétation des droits et des principes), de la Charte des droits fondamentaux de l'Union européenne[5].

La CJUE critique notamment que :

- la directive 2006/24/CE « *couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées de fonction de l'objectif de lutte contre les infractions graves* »[6] ;

- la directive 2006/24/CE « *ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence* »[7] ;

- en ce qui concerne les règles visant la sécurité et la protection des données conservées, la directive 2006/24/CE « *ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données* »[8].

Suite à l'arrêt précité, le Ministre de la Justice a sollicité l'avis de la CNPD sur la conformité de la loi modifiée du 30 mai 2005 et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt de la CJUE du 8 avril 2014. Dans son avis du 13 mai 2014, la Commission nationale a recommandé de modifier les dispositions nationales afin de les rendre conformes aux exigences posées par ledit arrêt[9]. La CNPD a réitéré ces

[5] CJUE, 8 avril 2014, *Digital Rights Ltd*, affaires jointes C-293/12 et C-594/12
[6] *Ibid.*, point 57
[7] *Ibid.*, point 60
[8] *Ibid.*, point 66
[9] Délibération n°214/2014 du 13 mai 2014 : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2014/Vorratsdatenspeicherung/214-2014-Deliberation-Ministere-Justice-avis-loi-modifiee-30-mai-2005-arret-CJUE-8-avril-2014-affaires-jointes-C-293-12-et-C-594-12-conservation-donnees.pdf

observations dans son avis relatif au projet de loi n°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005[10].

Par la suite, l'arrêt de la CJUE du 21 décembre 2016[11] a encore une fois mis en avant la nécessité de modifier les dispositions nationales en statuant que :

- l'article 15, paragraphe 1, de la directive 2002/58/CE « *doit être interprété en ce sens qu'il s'oppose à une règlementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* » ;

- l'article 15, paragraphe 1, de la directive 2002/58/CE « *doit être interprété en ce sens qu'il s'oppose à une règlementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union* ».

La CNPD estime dès lors qu'il y a lieu de de modifier et d'adapter le cadre législatif national afin d'assurer qu'il soit conforme à la jurisprudence de la CJUE.

Cette remarque vaut également pour l'article 7 de la loi du 5 juillet 2016 pour autant que le Service de renseignement de l'Etat puisse être amené à accéder aux données de trafic et de localisation conservées en vertu des articles 5 et 9 de la loi modifiée du 30 mai 2005.

En ce qui concerne le renvoi à l'article 88-1, paragraphe 1, du Code de procédure pénale, il serait opportun de clarifier si le projet de loi ne s'applique qu'à la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale, ou également aux autres mesures prévues par cette disposition, à savoir la sonorisation et la fixation d'images de certains lieux ou véhicules ainsi que la captation de données informatiques.

II. Définitions

L'article 2, point 4°, du projet de loi fournit une définition de la notion d'« opérateur » en renvoyant à la définition prévue par la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques selon laquelle l' « opérateur » est une entreprise notifiée qui fournit ou est autorisée à fournir un réseau de communications public ou une ressource associée.

---

[10] Délibération n°228/2015 du 19 juin 2015 : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2015/communications-electroniques/228_2015_Ministere-Justice_avis-projet-loi-modif-loi-communications-electroniques.pdf

[11] CJUE, 21 décembre 2016, *Tele2 Sverige AB*, affaires jointes C-203/15 et C-698/15

Ainsi, la notion d'« opérateur » est utilisée à l'article 3 du projet de loi tandis que les articles 4 et 5 emploient les notions d'« opérateurs de télécommunications » et de « fournisseurs d'un service de télécommunications », respectivement d'« opérateur des postes et télécommunications » .

La Commission nationale s'interroge pourquoi le projet de loi utilise des terminologies différentes.

Dans l'hypothèse où l'intention des auteurs du projet de loi serait d'utiliser les mêmes termes que ceux actuellement utilisés aux articles 67-1 du Code de procédure pénale et 7 de la loi du 5 juillet 2016, la Commission nationale se permet de renvoyer à son avis relatif au projet de loi n°6921 dans lequel elle a recommandé que la terminologie utilisée dans le Code d'instruction criminelle soit alignée sur celle d'ores et déjà utilisée dans la législation européenne et nationale[12].

En effet, la loi modifiée du 30 mai 2005, qui transpose plusieurs directives européennes, fait état d'opérateurs (de réseau) et de fournisseurs de services (de communications électroniques).

La CNPD suggère dès lors d'utiliser une terminologie uniformisée dans les différents textes.

III. Plateforme commune de transmission électronique sécurisée

A titre liminaire, la Commission nationale constate que la numérotation des paragraphes de l'article 3 du projet de loi semble erronée. Dans la suite de cet avis, elle utilisera une numérotation continue des paragraphes.

A. Quant à la qualification de responsable du traitement et de sous-traitant

L'article 3, paragraphe 2, du projet de loi dispose que la plateforme est hébergée auprès du Centre des technologies de l'information de l'Etat (ci-après : « le CTIE ») qui en assure la gestion opérationnelle.

Le paragraphe 3 du même article poursuit que le CTIE a la qualité de sous-traitant sans toutefois préciser quelle(s) autorité(s) est/sont à considérer comme responsable du traitement.

Dans le commentaire des articles, les auteurs du projet de loi indiquent que « *[l]es autorités judiciaires et le Service de renseignement de l'Etat sont responsables du traitement pour chaque donnée à caractère personnel qui les concerne* ». La Commission nationale estime que cette formulation peut prêter à confusion.

En effet, la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale (ci-après : « la loi du 1er août 2018 »), transposant la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités

[12] Délibération n°147/2016 du 12 février 2016, point 1 : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2016/lutte-terrorisme/147-2016-PL6921.pdf

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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, définit le responsable du traitement comme « *l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* ».

La personne concernée, par contre, désigne la personne physique identifiée ou identifiable à laquelle les données à caractère personnel se rapportent[13]. Il ne paraît dès lors pas approprié de prévoir que les autorités judiciaires et le Service de renseignement de l'Etat sont responsables du traitement pour les données qui les « concernent ». La CNPD comprend que chaque organisme est responsable pour la partie du traitement de données qui le concerne.

Le sous-traitant, quant à lui, est défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* »[14]. L'article 21 de la loi du 1er août 2018 traite plus particulièrement des relations entre le responsable du traitement et le sous-traitant.

La détermination du responsable du traitement revêt une importance particulière dans la mesure où il incombe notamment au responsable du traitement d'assurer le respect des principes énumérés à l'article 3 de la loi du 1er août 2018 et d'assurer les droits des personnes concernées conformément aux articles 11 et suivants de la loi du 1er août 2018.

La Commission nationale préconise partant que le projet de loi détermine clairement quelle(s) autorité(s) agi(ssen)t en tant que responsable du traitement. L'article 20 de la loi du 1er août 2018 prévoit d'ailleurs la possibilité que plusieurs autorités compétentes agissent comme responsables conjoints du traitement.

B. Quant aux éléments transmis aux opérateurs

Il ressort de l'article 3, paragraphe 4, du projet de loi et du commentaire y afférent que les opérateurs ne se voient plus communiquer les décisions ordonnant les mesures de repérage, de contrôle ou de surveillance, mais uniquement les éléments et informations techniques nécessaires à l'exécution des mesures.

La Commission nationale regrette que le projet de loi ne précise pas davantage quels éléments et informations techniques seront transmis par les autorités judiciaires et le Service de renseignement de l'Etat.

Par ailleurs, la Commission nationale se demande si le fait de ne plus communiquer l'ordonnance elle-même ne porte pas indûment atteinte au droit des opérateurs de former, le cas échéant, un recours contre les décisions ordonnant les mesures de repérage, de contrôle ou de surveillance.

[13] Article 2, paragraphe 1, point 1°, de la loi du 1er août 2018
[14] Article 2, paragraphe 1, point 9°, de la loi du 1er août 2018

C. Quant aux fichiers de journalisation des accès

Selon l'article 3, paragraphe 5, du projet de loi, « *[l]es informations relatives aux transmissions visées au paragraphe (4), à la personne ayant procédé à la consultation, aux informations consultées, aux critères de recherche, à la date et l'heure de la consultation ainsi qu'au motif de consultation sont conservées 12 mois à compter du jour où la mesure a été exécutée* ».

Le commentaire des articles précise que ces fichiers de journalisation des accès (ci-après : « log files ») sont nécessaires à la vérification de la légalité des opérations effectuées.

La Commission nationale se félicite que le projet de loi prévoit le principe du contrôle de l'accès aux données par le biais de la journalisation. Elle s'interroge toutefois si la durée de conservation prévue au projet de loi est conforme aux exigences posées par la CJUE dans son arrêt du 7 mai 2009[15].

En effet, les personnes concernées ont, en vertu du droit d'accès, notamment le droit d'obtenir du responsable du traitement des informations relatives aux destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées.

Dans l'affaire ayant donné lieu à l'arrêt précité du 7 mai 2009, la personne concernée désirait connaître l'identité des personnes tierces auxquelles des informations la concernant avaient été communiquées au cours des deux années précédant sa demande ainsi que le contenu de l'information qui leur a été transmise. Il ressort de l'arrêt précité que les communications des données sont enregistrées selon un système automatisé mais que les données demandées par la personne concernée, antérieure à l'année précédant sa demande, ont été automatiquement effacées, ce qui serait conforme à la législation nationale applicable.

Selon la CJUE, « *[i]l appartient aux Etats membres de fixer un délai de conservation de cette information [sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée] ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive [95/46/CE] et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement* »[16].

La Cour a conclu que « *[u]ne réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement* »[17].

Par ailleurs, l'effacement des log files après 12 mois est susceptible de rendre impossibles les poursuites judiciaires relatives à des violations du secret professionnel. En effet, tant les articles 67-1 et 88-4 du Code de procédure civile que l'article 7 de la loi du 5 juillet 2016

[15] CJUE, 7 mai 2009, affaire C-553/07
[16] *Ibid.*, point 70
[17] *Ibid.*

disposent que « *[t]oute personne qui, du chef de sa fonction, a connaissance de la mesure où y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal* ».

L'infraction prévue à l'article 458 du Code pénal est de nature correctionnelle de sorte que sa prescription est de 5 ans. La Commission nationale est partant d'avis que le délai de conservation des logs files devrait être porté de 12 mois à 5 ans.

D. Quant à l'effacement des résultats

L'article 3, paragraphe 5, du projet de loi précise encore que les informations reçues des opérateurs sont effacées dès confirmation de leur réception par l'autorité judicaire ou le Service de renseignement de l'Etat et qu'elles ne sont conservées sur la plateforme que le temps nécessaire à la transmission aux autorités requérantes.

Selon le commentaire des articles, ce mécanisme a pour but d'empêcher que la plateforme devienne un « annuaire » de toutes les demandes effectuées dans la mesure où elle ne sert qu'à transmettre les décisions et les résultats.

La Commission nationale se demande pourquoi le projet de loi ne prévoit que l'effacement des résultats transmis par les opérateurs et non pas l'effacement des demandes transmises par les autorités judiciaires ou le Service de renseignement de l'Etat.

En tout état de cause, l'effacement des résultats de la plateforme ne devrait pas compromettre la vérification de la légalité des opérations effectuées par le biais des logs files.

E. Quant à l'absence de règles de sécurité

Quand bien même le titre du projet de loi contient le terme « sécurisée », il ne prévoit pas, à part le mécanisme des logs files, de règles de sécurité destinées à protéger les traitements de données effectués par le biais de la plateforme.

Certes, l'article 28 de la loi du 1er août 2018 oblige le responsable du traitement et le sous-traitant de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Cependant, cette disposition laisse une marge de manœuvre beaucoup trop grande et n'est pas suffisante au vu du risque que ce traitement présente.

En l'espèce, il faudrait assurer un niveau de sécurité particulièrement élevé. Etant donné que la protection de la vie privée constitue une matière réservée à la loi[18], l'essentiel du cadrage normatif doit figurer dans la loi.

Il paraît dès lors souhaitable de voir compléter le projet de loi par des dispositions relatives aux obligations spécifiques de sécurité en tenant compte de la nature des données et du risque d'atteinte à la vie privée des citoyens.

[18] Article 11, paragraphe 3, de la Constitution

A cet égard, la Commission nationale entend d'ores et déjà rendre attentifs les auteurs du projet de loi que la mise en place de mesures de sécurité techniques et organisationnelles devrait tenir compte des risques suivants:

- Risque d'interception des messages

  - Identification et authentification systématique de l'émetteur ainsi que du récepteur pour chaque message échangé ;
  - Encryptage du canal de communication ainsi que du message échangé ;
  - Minimisation de tout risque d'écoute de la ligne de communication (*wiretapping*) en considérant en particulier le recours à des lignes non publiques sous contrôle de l'Etat.

- Risque d'un accès non légitime au système

  - Attribution nominative des accès sur base d'un processus formel et documenté dans le respect rigoureux du principe du *need-to-know need-to-do* ;
  - Revue régulière, systématique et documentée et au moins annuelle de l'ensemble des accès ainsi que des changements d'accès qui ont eu lieu sur la période ;
  - Définition des accès avec un niveau de granularité suffisant pour limiter l'accès à chaque émetteur de message afin de n'avoir accès uniquement qu'au retour de ses propres requêtes ;
  - Accès au système sur base d'une authentification forte ;
  - Accès au système à travers des postes de travail sécurisés et installés dans des locaux sécurisés ;
  - Aucun accès à des données réelles et de manière lisible par le personnel en charge pour développer, opérer, maintenir ou faire évoluer la plateforme ;
  - Sécurité des clé d'encryptage utilisées ;
  - Pertinence et le cas échéant remplacement ou mise à jour des algorithmes d'encryptage utilisés sur la plateforme.

- Risque d'une utilisation illégitime du système

  - Pas de possibilité de reconstruire ou de donner des indications substantielles sur le contenu des messages transmis en utilisant le traçage des opérations techniques et métier (*logs files*) ;
  - Pas de possibilité pour les utilisateurs métier ou technique de modifier les logs techniques et métier ;
  - Suppression sur les systèmes de l'opérateur des messages (requêtes ou réponses) transmis à l'opérateur ou envoyés par ce dernier dès réception respectivement envoi ;

- Détection d'anomalies ou d'abus métier et techniques à travers des revues régulières systématiques et documentées des logs ;
- Pas d'atteinte par le plan de backup aux durées de rétention des données définies ;
- Formation des utilisateurs ainsi que des opérateurs concernant le fonctionnement et leurs responsabilités spécifiques par rapport à la plateforme;
- Sensibilisation des utilisateurs ainsi que des opérateurs concernant les limites d'utilisation des données, notamment les limites de possibilité de croisement des messages entre eux.

F. Quant à l'obligation d'effectuer une analyse d'impact relative à la protection des données

L'article 26 de la loi du 1er août 2018 prévoit que le responsable du traitement doit effectuer préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques.

Même si les traitements de données effectués par les autorités judiciaires et le Service de renseignement de l'Etat au titre du projet de loi ne tombent pas dans le champ d'application du RGPD, il y a lieu de noter que ses considérants 92 et 93 disposent ce qui suit :

« *Il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.*

Au moment de l'adoption du droit d'un État membre qui fonde l'exercice des missions de l'autorité publique ou de l'organisme public concernés et qui règlemente l'opération ou l'ensemble d'opérations de traitement spécifiques, les États membres peuvent estimer qu'une telle analyse est nécessaire préalablement aux activités de traitement. »

Il y a dès lors lieu d'examiner en amont de la mise en place de la plateforme si une analyse d'impact relative à la protection des données s'avère nécessaire ou non.

IV. Modification du Code de procédure pénale et de l'article 7, paragraphe 3, alinéa 1, de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

Les auteurs du projet de loi expliquent dans l'exposé des motifs que le régime actuellement applicable pose des problèmes de confidentialité considérables en ce que « *la plupart du*

temps, les OPJ ou les membres du Service de renseignement de l'Etat notifient les décisions dans un guichet ou local non adapté de l'opérateur qui n'est pas équipé pour garantir la confidentialité nécessaire. Les ordonnances sont répertoriées dans un classeur non autrement sécurisé et se trouvent à la portée d'une bonne partie des employés. La protection des données, la protection de la vie privée et le caractère confidentiel de l'enquête sont dès lors menacées. »

C'est dans ce souci que la création de la plateforme a comme objectif principal d'améliorer la protection des données à caractère personnel des personnes faisant l'objet de mesures de repérage, de surveillance ou de contrôle.

Comme relevé au point III. E du présent avis, la Commission nationale n'est actuellement pas en mesure de l'apprécier, faute de plus amples précisions dans le projet de loi. Dans ce contexte, elle se pose par ailleurs la question de savoir pourquoi, au regard des déficiences du système actuel et des avantages de la plateforme mis en avant dans l'exposé des motifs, le projet de loi ne rend pas le recours à cette plateforme obligatoire.

Selon l'exposé des motifs, le projet de loi ne compte pas faire de la notification par voie électronique moyennant la plateforme commune une obligation. Cela est corroboré par les articles 4 et 5 du projet de loi selon lesquels « *[l]es éléments et informations techniques nécessaires (...) sont communiqués [notifiés] y compris par voie électronique sécurisée au travers de la plateforme (...)* ».

S'il ressort clairement du projet de loi que la transmission par les autorités judiciaires et le Service de renseignement de l'Etat aux opérateurs peut également se faire par d'autres moyens, il semble toutefois que les opérateurs soient obligés de transmettre les résultats au travers de la plateforme, tout au moins en ce qui concerne l'article 67-1 du Code de procédure pénale et l'article 7, paragraphe 3, de la loi du 5 juillet 2016.

En effet, le projet de loi prévoit de modifier le paragraphe 2 de l'article 67-1 en ce sens qu'il disposera que les opérateurs de télécommunications et les fournisseurs d'un service de télécommunications « *transmettent les résultats de cette exécution au moyen de la même plateforme dans les meilleurs délais* », sans faire de distinction selon le moyen par lequel la requête leur est parvenue.

En ce qui concerne l'article 7, paragraphe 3, de la loi du 5 juillet 2016, se pose également la question de savoir si les résultats doivent être transmis obligatoirement par la plateforme, peu importe le moyen par lequel la requête a été adressée, ou s'il y a lieu de suivre un « parallélisme des formes ».

L'article 88-4, paragraphe 1, du Code de procédure pénale, tel que modifié par le projet de loi, ne contient par contre aucune indication quant au moyen par lequel les résultats sont à transmettre. Il est simplement mentionné que chaque « *opérateur des postes et télécommunications* » tient un registre spécial dans lequel sont inscrits les éléments et les informations techniques notifiés et les suites qui leur sont données.

Au regard des fortes réserves que les auteurs du projet de loi ont exprimé à l'égard des « classeurs » tenus actuellement par les opérateurs et répertoriant les ordonnances, la Commission nationale s'interroge sur l'utilité de ce registre spécial. De plus, le projet de loi ne

contient pas d'explications quant à l'utilisation du terme « opérateur des postes et télécommunications ». A cet égard, la Commission nationale se permet de renvoyer à ses développements sous le point II. du présent avis.

L'article 88, paragraphe 3, du Code de procédure pénale reste inchangé en ce qu'il prévoit que « *[l]es télécommunications, correspondances postales, images, conversations ou données enregistrées ou interceptées sont remises sous scellés et contre récépissé au juge d'instruction qui dresse procès-verbal de leur remise* ».

La Commission nationale se pose la question de savoir comment cette disposition s'articule avec la transmission électronique au travers de la plateforme telle que prévue par le projet de loi.

Par ailleurs, il n'est pas clair pour la Commission nationale de quelle manière s'opérera la transmission, par le biais de la plateforme, des résultats de la surveillance et du contrôle de « correspondance postale » visée dans le prédit article 88, paragraphe 3, du Code de procédure pénale.

En outre, l'article 7, paragraphe 1, de la loi du 5 juillet 2016 vise la surveillance et le contrôle de la communication électronique et de la « correspondance postale ».

Le paragraphe 3, alinéa 1, dudit article, tel que modifié par le projet de loi, ne mentionne toutefois que la transmission des éléments et information techniques nécessaires à l'exécution des mesures de surveillance et de contrôle aux opérateurs de « télécommunications » et aux fournisseurs d'un service de « télécommunications ». Il n'est pas clair pour la Commission nationale par quel biais les requêtes concernant la surveillance et le contrôle de la « correspondance postale » seront transmises aux opérateurs concernés[19], respectivement de quelle manière les résultats sont à transmettre.

De plus, l'article 7, paragraphe 3, alinéa 3, de la loi du 5 juillet 2016 reste inchangé en ce qu'il dispose que « *[l]es correspondances sont mises sous scellés et remises contre récépissé au SRE, qui fait copier les correspondances pouvant servir à ses investigations et renvoie les écrits qu'il ne juge pas nécessaire de retenir aux opérateurs qui les font remettre au destinataire* ».

La Commission nationale s'interroge sur l'articulation de cette disposition avec la transmission électronique au travers de la plateforme telle que prévue par le projet de loi.

[19] La même remarque vaut pour l'article 88-4 du Code de procédure pénale

Ainsi décidé à Esch-sur-Alzette en date du 5 juin 2019.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire