Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal pris en exécution de la future loi portant réorganisation du Service de Renseignement de l'Etat et au projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité

Délibération n° 639/2016 du 13 juillet 2016

Conformément à l'article 32 paragraphe (3) lettre (e) 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 modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou «la CNPD ») a notamment pour mission d'«*être demandée en son avis sur 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 deux courriers du 8 juin 2016, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État, règlement à prendre en exécution de la future loi portant réorganisation du Service de Renseignement de l'Etat votée à la Chambre des Députés en date du 9 juin 2016 (projet de loi n° 6675) et au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, règlement à prendre en exécution de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

La Commission nationale passe en revue les articles qui donnent lieu à observations.

I. Le projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État

Ad article 3

L'article 3 aborde la question des données à caractère personnel que le Service de renseignement est en droit de traiter.

La Commission nationale rappelle dans ce contexte que l'*avant-projet de règlement grand-ducal portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'Etat* soumis à la CNPD pour avis en 2013 comportait en son article 5 une longue énumération des catégories de données pouvant être traitées. A ce titre, la CNPD avait formulé un grand nombre d'observations relatives à cette énumération[1] qu'elle souhaite réitérer pour les besoins du présent avis. Elle

[1] Avis de la Commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et à l'avant-projet de règlement grand-ducal pris en exécution de

s'étonne que l'actuel projet de règlement sous avis ne contienne plus cette énumération des catégories de données.

Le règlement grand-ducal à prendre en vertu de l'article 10 paragraphe (1) de la future loi portant réorganisation du Service de Renseignement de l'Etat est pourtant censé donner des précisions relatives aux traitements de données qui peuvent être effectués par le Service de renseignement. Or, la formulation utilisée (« toutes données... ») à l'article 3 est à tel point vague et générale qu'on peut se demander s'il y a des limites quant à l'étendue de la collecte des données ou quelles sont les données qui ne peuvent *pas* être traitées par le Service de renseignement. La CNPD estime que l'article 3 dans sa teneur actuelle ne satisfait pas à l'article 8 paragraphe 2 de la Convention européenne des droits de l'homme et des libertés fondamentales qui exige que toute ingérence dans la vie privée par une autorité publique doit nécessairement reposer sur une base légale ou réglementaire suffisamment précise (voir aussi les développements à l'article 9 in fine du présent avis).

Pour ce qui est plus précisément des données sensibles mentionnées à la lettre c) de l'article 3, la Commission nationale regrette que le texte sous avis permette leur traitement d'une manière aussi généralisée. Rappelons que sont visés «*les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions, religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques*»[2]. La CNPD s'interroge sur la nécessité du traitement des données relatives à la santé et à la vie sexuelle est excessif. L'avant-projet de règlement soumis à la CNPD pour avis en 2013 excluait expressément le traitement de données relatives à la santé et à la vie sexuelle.

Ad article 4

Selon l'article 4 du projet de règlement sous avis, il «*sera procédé à un réexamen de la nécessité de conserver les données traitées au plus tard tous les dix ans*».

La Commission nationale considère que ce délai de dix ans est excessivement long, eu égard notamment au caractère en partie très sensible des données et eu égard au fait que les personnes concernées ne sauront normalement pas qu'elles font l'objet d'un traitement de données à caractère personnel. Rappelons que l'avant-projet de règlement soumis à la CNPD pour avis en 2013 prévoyait un délai de réexamen de cinq ans seulement et que la CNPD plaidait dans son avis du 28 juin 2013 pour un délai de trois ans.

La CNPD salue cependant que ce délai commence à courir à partir du premier enregistrement d'une donnée à caractère personnel concernant la personne visée en relation avec la finalité ayant donné lieu au traitement des données concernées.

Ad article 7

L'article 7 traite des autorisations d'accès à accorder par le Directeur du Service de renseignement.

---

l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, délibération n° 274/2013 du 28 juin 2013
http://www.cnpd.public.lu/fr/decisions-avis/2013/sre/index.html

[2] article 6 paragraphe (1) la loi modifiée du 2 août 2002

Il serait préférable que les agents bénéficiant d'une autorisation d'accès n'aient pas d'office accès à l'intégralité de la partie active, mais qu'il soit précisé dans le règlement que les droits d'accès soient limités aux besoins de chaque agent eu égard à ses missions en fonction de critères objectifs définis dans une procédure interne.

Il serait par ailleurs indiqué de préciser dans le règlement qu'en cas de réaffectation interne d'un agent ou d'un changement de ses missions, les autorisations devront être adaptées ou retirées en fonction du nouveau poste ou des nouvelles missions.

Enfin, même si cela semble aller de soi, il ne serait pas inutile de préciser que toute autorisation devrait être retirée quand un agent quitte le Service de renseignement de manière temporaire ou définitive. A ce titre, la CNPD renvoie au rapport annuel de Autorité de contrôle spécifique "Article 17" pour les années 2014 et 2015 qui aborde la question des mutations entre les services de police d'un côté et le Service de renseignement de l'autre.[3]

Ad article 8

Selon l'exposé des motifs, « *une attention particulière a été portée à la journalisation des accès aux données à caractère personnel pour un meilleur suivi et contrôle des consultations ou des traitements effectués par les différents agents du SRE* ».

Or, l'article 8 paragraphe (2) ne fait que poser le principe de la conservation des données de journalisation. La Commission nationale estime qu'il est nécessaire de prévoir, dans le texte du règlement grand-ducal, une obligation de contrôler, sur base régulière, les données de journalisation (telles que définies à l'article 9 du projet de règlement grand-ducal), afin de détecter d'éventuels abus.

En outre, la Commission nationale recommande de préciser la procédure prévue pour enregistrer et traiter les données de journalisation mentionnée dans l'article 8 paragraphe (2) afin de garantir une transparence accrue de la gestion de ces données. Il serait important :

- de mettre en œuvre des mesures (par exemple de type cryptographique) pour garantir l'intégrité du contenu de la journalisation : le contenu ne doit pas pouvoir être manipulé, et plus particulièrement par la possibilité de modification ou de suppression des enregistrements ;
- de garantir la confidentialité (par exemple de type cryptographique) du contenu de la journalisation.

Par ailleurs, la Commission nationale considère qu'il est primordial de conserver des sauvegardes des fichiers contenant les données de journalisation, afin de prévenir la perte de la continuité et de la disponibilité de ces données (par exemple, suite à leur suppression par un attaquant). Enfin, il est important que des protocoles de sécurité répondant à l'état de l'art soient utilisés pour garantir la confidentialité et l'intégrité des données de journalisation lors de leur transfert du système de conservation de ces données vers le système de sauvegarde.

---

[3] Rapport annuel de Autorité de contrôle spécifique "Article 17" pour les années 2014 et 2015, page 10 en bas et page 15
http://www.cnpd.public.lu/fr/publications/rapports/groupe_article17/rapport_1415.pdf
cf aussi : Scéance publique de la Chambre des Députés du 10 mai 2016
http://visilux.chd.lu/ArchivePage/video/1718/sequence/75133.html

Ad article 9

La Commission note avec satisfaction que sont établis des fichiers de journalisation comprenant, outre les informations relatives à l'agent ayant procédé au traitement, la date, l'heure et aussi les informations relatives au motif de l'accès conformément à l'article 10 du projet de loi n° 6675.

Elle estime cependant que le délai de conservation des fichiers de journalisation de 3 ans est insuffisant, eu égard au caractère partiellement sensible des données, mais également eu égard aux antécédents en matière de traitements de données du Service de renseignement non conformes à la loi.

Dès lors, la Commission nationale suggère que ce délai soit porté à 5 ans. Il convient de relever que la prescription des délits, et notamment des infractions à la législation sur la protection des données (par exemple l'accès non autorisé ou abusif à des données), est de 5 ans. Or, une conservation des fichiers de journalisation pendant seulement 3 ans risquerait, dans de nombreux cas, de rendre impossible de fait des poursuites judiciaires au-delà de cette durée de 3 ans.

La Commission nationale note encore que article 12 de l'avant-projet de règlement lui soumis pour avis en 2013 prévoyait la communication de données aux autorités judiciaires, aux autorités de police et aux administrations, ainsi qu'aux organismes de renseignement et de sécurité étrangers. Si le présent projet de règlement sous avis ne contient plus de dispositions à ce sujet, le principe de ces communications a cependant été maintenu au niveau de la loi avec l'article 9 de la future loi portant réorganisation du Service de Renseignement de l'Etat. La CNPD réitère à ce sujet sa demande formulée en 2013 que les communications de données en question devraient être retraçables et faire l'objet d'une documentation.

Enfin, la CNPD regrette que le gouvernement n'ait pas profité de l'occasion pour inclure, dans le projet de règlement grand-ducal sous avis, des précisions relatives à la question de l'accès par le Service de renseignement à des systèmes informatiques prévu à l'article 8 paragraphe (1) lettre c) de la future loi portant réorganisation du Service de Renseignement de l'Etat. En effet, cette mesure de surveillance pouvant être mis en œuvre par le Service de renseignement porte par nature une atteinte grave au droit au respect de la vie privée et à la protection des données à caractère personnel des personnes en faisant l'objet. Une telle atteinte ne saurait être admise que si elle apparaît strictement nécessaire au but poursuivi et si des garanties suffisantes sont prévues, de nature à garantir la proportionnalité des dispositifs de surveillance mis en œuvre. En particulier, la Commission nationale rappelle que de tels mesures ou dispositifs de surveillance doivent, conformément à l'article 8 paragraphe 2 de la Convention européenne des droits de l'homme et des libertés fondamentales, ainsi qu'à la jurisprudence de la Cour de Strasbourg en la matière, reposer sur une base légale suffisante et être mis en œuvre dans des conditions permettant d'assurer un juste équilibre entre l'ingérence dans la sphère privée de la personne surveillée à son insu et les troubles à l'ordre public susceptibles de résulter d'activités qui pourraient menacer la sécurité nationale.

La CNPD renvoie à ce sujet à ses développements exhaustifs, exposés au point 7.3. dans son avis (délibération n° 147/2016) du 12 février 2016 relatif au projet de loi n°6921 portant adaptation de la procédure pénale face aux besoins liées à la menace terroriste[4].

Il résulte de ce qui précède qu'il est primordial que le gouvernement prévoit dans le projet de règlement grand-ducal sous examen ou dans un projet de règlement grand-ducal séparé des règles précises quant à la question soulevée ci-avant, afin de satisfaire aux exigences de la Convention européenne des droits de l'homme et des libertés fondamentales ainsi qu'à la jurisprudence de la Cour de Strasbourg en la matière.

II. Le projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité

A titre liminaire, la CNPD note que son avis a été demandé sur le projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, mais qu'elle n'a pas été saisie pour avis en ce qui concerne le projet de loi n° 6961 portant modification 1. de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2. du Code pénal.

Ad article 3

La CNPD regrette que le texte ne donne aucune précision sur l'origine des données. Le texte devrait au moins faire une distinction entre les données que le demandeur d'une habilitation doit fournir lui-même et celles qui sont collectées à partir d'autres fichiers étatiques ou encore par d'autres moyens de recherche.

En ce qui concerne les catégories de données pouvant faire l'objet d'un traitement, l'article ne contient pas d'énumération explicite des catégories de données à l'image de l'article 5 de l'avant-projet de règlement lui soumis pour avis en 2013, mais ne fait que renvoyer aux critères d'appréciation de l'article 24 bis projeté de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité tel que prévu par le projet de loi n° 6961 sans pour autant fournir davantage de détails.

En ce qui concerne par exemple des données relatives à « *la mise en accusation dans des affaires judiciaires, y compris des affaires de mœurs* », on peut se demander à partir de quel stade (enquête préliminaire, instruction, décision de renvoi de la chambre du conseil) on peut considérer quelqu'un comme « mis en accusation » au sens de l'article en question. On pourrait aussi se poser la question si l'utilisation du terme « accusation » se réfère de manière spécifique aux affaires criminelles ou aux affaires pénales en général. Il semble également étonnant qu'on se réfère de manière expresse aux affaires de mœurs.

Pour ce qui est des données relatives à l'insolvabilité, il se pose également la question de savoir de quelles données il s'agit précisément et quelle est leur source. Fait-on référence à des procédures judiciaires civiles liées au surendettement ? Or, si on accorde à l'ANS un accès aux données relatives à ces procédures, il faudrait le prévoir de manière plus explicite à l'article 22

[4] http://www.cnpd.public.lu/fr/decisions-avis/2016/lutte-terrorisme/147-2016-PL6921.pdf

de la loi du 15 juin 2004 dans sa version du projet de loi n°6961. Le Luxembourg ne dispose pas non plus de banque de données publique contenant des données relatives à la solvabilité à l'image de la Centrale des crédits aux particuliers de la Banque nationale de Belgique ou des Fichiers d'incident bancaire de la Banque de France. Et même si une telle banque de donnée existait dans le futur, elle devrait être citée à l'article 22 de la loi du 15 juin 2004 dans sa version du projet de loi n°6961 afin que l'ANS puisse y avoir accès. Est-ce que les données pourraient provenir par exemple de banques ? Mais dans ce cas, le secret bancaire ne pourrait-il pas être opposé à l'ANS ? Ou ces données seraient-elles simplement fournies par la personne concernée avec tous les risques de fiabilité que cela comporterait.

Ces incertitudes soulèvent encore une fois l'importance de la détermination par voie règlementaire de l'origine des données.

Ad articles 7, 8 et 9

La CNPD renvoie à ses observations faites ci-dessus relatives aux articles 7, 8 et 9 du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État.

Enfin, la CNPD tient encore à faire quelques observations relatives au droit d'accès.

A défaut de dispositions spécifiques, les règles de l'article 17 de la loi modifiée du 2 août 2002 s'appliqueront, règles ne permettant qu'un droit d'accès «indirect» extrêmement limité.

Or, la question des habilitations de sécurité ne saurait être traitée sur un pied d'égalité avec des mesures policières ou des mesures de services de renseignements qui visent à élucider respectivement à prévenir des infractions pénales en partie très graves et où un droit d'accès direct risquerait d'anéantir les efforts des autorités en question.

La CNPD est dès lors à se demander s'il ne serait pas plus approprié d'introduire, par voie légale, un droit d'accès direct selon les règles de droit commun de l'article 28 de la loi modifiée du 2 août 2002 à l'instar d'autres pays. En cas d'application du droit d'accès direct de droit commun, les exceptions prévues par l'article 29 de la loi modifiée du 2 août 2002 s'appliqueraient le cas échéant. Alternativement aux exceptions de l'article 29, on pourrait, en cas de besoin, prévoir des exceptions spécifiques au droit d'accès en matière d'habilitations de sécurité. A titre d'exemple de disposition prévoyant un droit d'accès (direct) assorti d'exceptions, on pourrait se référer à l'article 23 du *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG)* allemand[5].

[5] http://www.gesetze-im-internet.de/s_g/__23.html

Quel qu'il en soit, d'éventuelles dispositions relatives à un droit d'accès direct devraient au moins avoir une base légale dans la future loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (projet de loi n°6961), le règlement grand-ducal d'exécution pouvant tout au plus compléter ou préciser les dispositions de la loi.

Ainsi décidé à Esch-sur-Alzette en date du 13 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif