Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 08/2022 du 21 janvier 2022

Objet : Avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité (CO-A-2021-256)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité ») ; Présent.e.s. :Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Frank Robben ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA ») ;

Vu le 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 « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis du Premier Ministre, Alexander De Croo, reçue le 30 novembre 2021 ;

Vu les informations complémentaires reçues en date du 14 décembre 2021 ;

Émet, le 21 janvier 2022, l'avis suivant :

I. Objet et contexte de la demande

1. En date du 30 novembre dernier, le Premier Ministre a sollicité l'avis de l'Autorité sur l'avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité (ci-après « l'avant-projet de loi »).

2. Cet avant-projet de loi vise à exécuter le Règlement (UE) 2019/881 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications (TIC) (ci-après le « Règlement cybersécurité »).

3. Ce Règlement cybersécurité vise à renforcer la confiance dans le secteur des TIC en définissant un cadre européen de certification de cybersécurité, qui fixe des règles horizontales pour le développement de schémas de certification de cybersécurité pour différentes catégories de produits[1], services[2] et processus[3] TIC. L'ENISA a la charge de la préparation des schémas de certification qui seront ensuite adoptés par la Commission européenne au moyen d'actes d'exécution. Un schéma européen de certification de cybersécurité est, selon le Règlement Cybersécurité, « *un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, services TIC ou processus TIC spécifiques* ». Chaque schéma de certification spécifiera, entre autres, le type ou les catégories de produits, services et processus TIC couverts, l'objet, les normes et les méthodes d'évaluation. Les certificats de cybersécurité européen, délivrés par les organismes d'évaluation de la conformité accrédités par les organismes nationaux d'accréditation, attesteront qu'un produit TIC, service TIC ou processus TIC a été évalué en qui concerne sa conformité aux exigences de sécurité spécifique fixées dans un schéma européen de certification de cybersécurité. Le Règlement cybersécurité définit 3 niveaux d'assurance, qui sont corrélés à des niveaux de risques différents. Il s'agit des niveaux suivants : élémentaire, substantiel et élevé.

4. Sauf disposition contraire du droit de l'Union européenne ou du droit national d'un État membre, une certification ou une déclaration de conformité est volontaire. La Commission européenne évaluera à des intervalles planifiés la nécessité de rendre des certificats obligatoires. Le Règlement cybersécurité prévoit la possibilité de se faire certifier ou de procéder à une déclaration de

[1] Définis par le Règlement cybersécurité comme étant un *« élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information* ».

[2] Définis par le Règlement cybersécurité comme étant un « *service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information* ».

[3] Définis par le Règlement cybersécurité comme étant un « *ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance* ».

conformité. Un certificat est délivré par un organisme d'évaluation de la conformité indépendant et accrédité. Une déclaration de conformité est délivrée sous la responsabilité du fabricant ou fournisseur TIC au moyen d'une autoévaluation. Tout schéma de certification précise si une telle déclaration de conformité est permise ou pas et l'auto-évaluation est limitée au niveau d'assurance « élémentaire ».

5. Les Etats membres doivent en exécution de ce Règlement désigner la ou les autorités nationales de certification de cybersécurité, qui délivreront des certificats, ou encore qui assurent la supervision et le contrôle de la bonne application des règles par les différents acteurs (fabricants, fournisseurs et prestataires de produits et services TIC titulaires d'un certificat ou ayant émis une déclaration de conformité et organismes d'évaluation de la conformité). De plus, les Etats membres doivent définir des règles spécifiques dans leur droit national pour assurer la bonne application de ce Règlement, par exemple concernant les sanctions ou le retrait de certificats. C'est l'objet de l'avant-projet de loi soumis pour avis.

II. Examen

Observations générales – Communications de données par les autorités en charge du contrôle du respect du Règlement cybersécurité et des schémas européens de certification de cybersécurité et protection de la clientèle (personnes physiques) des prestataires de services ICT contrôlés (ou des clients personnes physiques de cette clientèle dont les données sont reprises dans les services ICT contrôlés)

6. Le présent avis de l'Autorité ne vaut que pour autant que des traitements de données concernant des personnes physiques soient visés par les dispositions de l'avant-projet de loi. Les traitements de données qui devront être réalisés dans le cadre des contrôles requis par le Règlement cybersécurité pourront porter sur des données à caractère personnel au sens du RGPD lorsque les fabricants ou fournisseurs de produits TIC, les prestataires de services TIC ou de processus TIC titulaires ou demandeurs d'un certificat de conformité de cybersécurité européen seront des personnes physiques mais également lorsque le contrôle du respect des schémas de certification par les prestataires desdits services TIC certifiés impliquera le traitement de données à caractère personnel telles que les données de leurs clients personnes physiques ou des clients personnes physiques de leurs clients. Si l'on prend, à titre d'exemple, des services cloud[4] ; il est fréquent que les clients d'un prestataire de service cloud l'utilisent pour leurs propres traitements de données à

[4] Cf EUCS, candidate cybersecurity certification scheme for cloud services, december 2020, disponible sur le site de l'ENISA à l'adresse suivante https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/@@download/fullReport. Il y est prévu que « The EUCS scheme may cover any type of ICT service, provided that the ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface (ISO 17788) and that the ICT service aims at reaching the assurance level corresponding to one of the three levels « basic », « substantial » and « high » of the EUCSA as defined in the EUCS scheme.

caractère personnel ; lesquels peuvent porter sur des catégories particulières de données au sens du RGPD en fonction du domaine d'activité desdits clients (ex. un hôpital, un cabinet d'avocat ou encore une autorité publique en charge de mission de prévention et de détection d'infractions pénales).

7. Comme cela a été relevé par le Contrôleur européen à la protection des données dans un de ses avis récent sur la stratégie européenne en matière de cybersécurité et sur la directive SRI 2.0[5], « l*'article 5, paragraphe 1, point f), du RGPD a posé la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel. L'article 32 du RGPD définit plus précisément l'obligation – applicable tant aux responsables du traitement qu'aux sous-traitants – de garantir un niveau de sécurité approprié. Ces deux dispositions indiquent clairement que la sécurité est essentielle au respect de la législation européenne en matière de protection des données. C'est pourquoi (…) l'amélioration de la cybersécurité est essentielle à la sauvegarde des droits fondamentaux. y compris du droit au respect de la vie privée et à la protection des données à caractère personnel (…). Dans le même temps, (…) la poursuite des objectifs de cybersécurité peut donner lieu au déploiement de mesures qui constituent une ingérence dans les droits à la protection des données et au respect de la vie privée des personnes. Il convient donc de veiller à ce que toute limitation potentielle du droit à la protection de la vie privée et des données à caractère personnel réponde aux exigences de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, et en particulier qu'elle soit mise en œuvre par le biais d'une mesure législative, qu'elle soit à la fois nécessaire et proportionnée et qu'elle respecte le contenu essentiel du droit »*

8. Au regard de ces considérations, l'avant-projet de loi est problématique en raison des échanges de données qu'il prévoit en des termes très larges entre, d'une part, l'autorité nationale de certification de cybersécurité et les autres autorités qui seront désignées pour la réalisation des missions de contrôle prévues par le Règlement cybersécurité et, d'autre part, les autorités suivantes: les autorités judiciaires, les autorités sectorielles ou les services d'inspection visés respectivement à l'article 7, § 3 et § 5 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les autorités de surveillance de marché, l'autorité nationale d'accréditation, les services de sécurité publique, les services de police, les services de renseignement et l'autorité visée à l'article 7, § 4 de la du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

[5] Avis du CEPD 05/2021 sur la stratégie en matière de cybersécurité et la directive SRI 2.0, disponible sur le site du CEPD à l'adresse suivante https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en

9. Ces échanges posent question au vu de leur objet très large, tel qu'actuellement prévus par l'avant-projet de loi. A plusieurs reprises, il y est en effet prévu qu'ils ont lieu non seulement pour l'exercice des missions de services public consistant au contrôle du respect du Règlement cybersécurité et des schémas de certification européen de cybersécurité ou des déclarations de conformité réalisées en exécution dudit Règlement mais également pour l'application de toute autre disposition légale (sans préciser de quelle disposition légale il s'agit ; ce qui ne permet pas de vérifier si elle présente un lien clair avec le Règlement cybersécurité précité). Cela apparait disproportionné, non conforme au champ d'application de l'avant-projet de loi censé mettre en œuvre le règlement cybersécurité, selon les considérations générales de l'exposé des motifs.

10. De plus, ce défaut d'encadrement minimal desdits échanges risque de mettre à mal l'objectif de confiance dans les produits et services TIC certifiés que poursuit le Règlement européen cybersécurité étant donné que les données des clients (ou de la clientèle de ceux-ci) des prestataires services TIC contrôlés par l'autorité de certification de cybersécurité pourront, selon le libellé de l'avant-projet de loi, être collectées et utilisées par des services publics qui ne disposent pas de mission spécifique liée à la cybersécurité tels que par exemple les services de police ou les services de renseignement et ce, pour leur propres missions de prévention et de détection de n'importe quelles infractions pénales, d'enquêtes et de poursuites ou encore pour n'importe quelles mission de la Sûreté de l'Etat et du service général du Renseignement et de la Sécurité. Cette situation risque de constituer un frein à la promotion de services et produits ICT certifiés conformément au Règlement cybersécurité et, par voie de conséquence, à l'amélioration de sécurité de l'information dans ces domaines.

11. L'auteur de l'avant-projet de loi doit donc encadrer les échanges conformément au strict nécessaire et raisonnable au regard du champ d'application et des objectifs du Règlement cybersécurité. L'article 58.7.a du Règlement cybersécurité prévoit d'ailleurs que c'est uniquement en coopération avec les « *autres autorités compétentes de surveillance du marché* » que les autorités nationales de certification de cybersécurité doivent superviser et faire respecter les règles prévues dans les schémas européens de certification de cybersécurité et non n'importe quelle autorité publique. L'article 58.7.h de ce Règlement prévoit quant à lui que les autorités nationales de certification de cybersécurité « *coopèrent avec d'autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques*, *notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC, et processus TIC des exigences du présent règlement ou des exigences de schéma de certification de cybersécurité spécifiques* ». Le considérant 102 de ce Règlement précise à ce sujet que « *la Commission devrait faciliter ce partage d'informations grâce à la mise à disposition d'un système général de soutien à l'information électronique, par exemple, le système d'information et de communication pour la surveillance des marchés (ICSMS) et le système européen d'échange rapide sur les produits*

dangereux (RAPEX) déjà utilisés par les autorités de surveillance du marché en vertu du Règlement (CE) n°765/2008. » Cet exemple de signalement des alertes quant à la présence d'un produit ou d'un service non conforme à un schéma de certification cadre bien avec le cadre européen de certification de cybersécurité tel que décrit à l'article 46 du Règlement de cybersécurité. Lesdits échanges doivent, aux yeux de l'Autorité, donc se limiter à la réalisation de cet objectif et ne pas permettre l'application de n'importe quelle disposition légale. Ce partage d'informations sur le non-respect, par des produits TIC, services TIC et processus TIC, des exigences du Règlement Cybersécurité ou de certains schémas européens de certification de cybersécurité spécifiques ne nécessite pas, selon l'Autorité, de devoir échanger les données à caractère personnel que lesdits clients mettent à dispositions desdits prestaires dans le cadre de leur relation contractuelle.

12. Interrogé quant à ce qui justifie la mise en place d'échange de données avec les différentes autorités visées à l'article 6, §3 en projet, le délégué du Ministre a précisé ce qui suit :
    a. En ce qui concerne les autorités judiciaires *: « il apparaît nécessaire que les autorités judiciaires puissent solliciter ou être notifiées des informations en cas d'infractions pénales (fraudes liées à la délivrance, aux contrôles, aux sanctions et aux réclamations des certifications de cybersécurité ou d'infractions pénales prévues par les différentes législations sectorielles - dont la loi NIS) ».* A ce sujet, l'Autorité relève, tout d'abord, qu'à la lecture de l'avant-projet de loi les infractions au Règlement cybersécurité et aux schémas européens de certification ne sont pénalisées que par la modification du Code de droit économique et que c'est le livre XV de ce Code qui organise déjà les communications de données que l'inspection économique peut réaliser dans l'exercice de ses missions. Ensuite, l'article 29 du Code d'instruction criminelle (Cicr) prévoit déjà que « toute autorité constituée, tout fonctionnaire ou officier public (…) qui, dans l'exercice de ses fonctions acquerra la connaissance d'un crime ou d'un délit, sera tenu de donner avis sur-le-champ au procureur du Roi près le tribunal dans le ressort duquel ce crime ou ce délit aura été commis ou dans lequel l'inculpé pourrait être trouvé, et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. ». Il n'est pas nécessaire, voir contre-productif en termes de protection des données à caractère personnel, de répéter sans la modaliser, cette communication de données dans l'avant-projet de loi ; d'autant plus que l'article 29 du Cicr impose le respect de certaines formalités à ce sujet. L'Autorité recommande par conséquent la suppression de cet échange de l'avant-projet de loi.

    b. En ce qui concerne les autorités sectorielles (NIS)[6] *: « ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle des mesures de sécurité des réseaux et*

[6] Ainsi qu'il ressort des informations complémentaires, il s'agit des autorités suivantes :

systèmes d'informations (P.S.I., voir article 21 et suivants de la loi NIS), qui serait titulaire ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant ».

A ce sujet, l'Autorité comprend que ces autorités sectorielles, disposant de missions spécifiques en matière de sécurité de l'information, doivent être informées que les organisations dont elles contrôlent le respect des dispositions de la loi précitée du 7 avril 2019 (dite loi NIS) utilisent des services ou produits TIC certifiés dont le non-respect du schéma de certification a été mis en évidence par l'Autorité nationale de certification ou une autorité désignée en exécution de l'article 5,§2 de l'avant-projet de loi. A ce sujet, l'Autorité se demande si les mesures de retrait de certification -qui devraient par nature être soumises à des mesures de publicité – ne devraient pas être suffisantes à cet effet. Si cela ne devait pas être le cas (ce qu'il convient de justifier dans l'exposé des motifs), vu la caractère lié à la cybersécurité des missions des autorités de contrôle instituées en vertu de la loi NIS, l'Autorité considère que ces échanges apparaissent nécessaires mais

---

« Les autorités sectorielles visées à l'article 3, § 3 de l'avant-projet de loi sont les autorités visées à l'article 6, 2° de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après, « loi NIS »).

Il s'agit concrètement des autorités suivantes :

- *Désignées par la loi NIS :*
  - *La BNB (art. 95. de la loi NIS qui a inséré un article 36/47 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique).*
  - *La FSMA (art. 90 et 91 de la loi NIS ayant modifiés les art. 71 et 79 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers).*
  - *L'IBPT (art. 88. de la loi NIS qui a modifié l'art. 14, § 1er, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges).*
- *Désignées par l'annexe 1 de l'arrêté royal du 12 juillet 2019 (portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques) :*
  - *pour le secteur de l'énergie : le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des transports :*
    - *En ce qui concerne le secteur du transport, à l'exception du transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour le Transport, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
    - *En ce qui concerne le transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour la Mobilité maritime, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur de la santé : le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des fournisseurs de service numérique : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
- *Désignée par l'arrêté royal du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable :*
  - *le Comité national de sécurité pour la fourniture et la distribution d'eau potable »*

qu'il convient, en plus de définir la notion d' « *autorités sectorielles* » utilisée par l'avant-projet de loi (référence explicite aux autorités visées) et de déterminer clairement dans l'avant-projet de loi[7] les circonstances et modalités de ces communications de données par l'autorité nationale de certification de cybersécurité et les autorités désignées en exécution de l'article 5, §2 en projet ainsi que la finalité du traitement qui sera réalisé avec ces informations par lesdites autorités sectorielles. De plus, il conviendra alors aussi de prévoir la limitation des échanges relatifs au constat d'un manquement aux normes de sécurité de l'information dont ces autorités assurent le contrôle aux seules entités se trouvant sous la surveillance desdites autorités

c. En ce qui concerne les autorités de surveillance des marchés *: « Ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle portant sur les mesures de sécurité appliquées par les entités sur lesquelles elles ont une compétence de contrôle, qui serait titulaire ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant. »*

   Si ces autorités de surveillance des marchés disposent de missions spécifiques en matière de cybersécurité, ce qu'il appartient à l'auteur de l'avant-projet de loi de justifier, et si de telles communications quant à la certification des entités visées n'est pas déjà prévue par ailleurs, les communications visées apparaissent pertinentes et nécessaires mais il est renvoyé aux remarques précédentes sur les autorités sectorielles pour leur encadrement adéquat (désignation des seules autorités de surveillance disposant de telle compétence, limitation des échanges relatifs au constat d'un manquement aux normes de sécurité de l'information dont ces autorités de surveillance des marchés assurent le contrôle aux seules entités se trouvant sous la surveillance desdites autorités, …). A défaut, cette communication sera supprimée de l'avant-projet de loi.

d. En ce qui concerne les services de sécurité publique : *« Dans le cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou dans le cas où ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services.»*

[7] pour autant que ces précisions ne figurent pas déjà dans la loi NIS, ce qu'il appartient à l'auteur de l'avant-projet de loi de vérifier.

Interrogé quant aux autorités visées par cette notion de « *services de sécurité publique* », le délégué du Ministre a précisé qu'il s'agissait des autorités suivantes : *« SPF Intérieur, Bruxelles Prévention et Sécurité, Service public de Wallonie, Vlaamse Overheid, Administrations publiques locales (provinces et communes), Gouverneurs, OCAM ».*

Outre l'absence de définition dans l'avant-projet de la loi de la notion de service de sécurité publique (qu'il convient de pallier en se référant explicitement auxdites autorités ou plutôt, dans la plupart des hypothèses, à leur service compétent en matière de sécurité publique), le défaut d'encadrement minimal de ces échanges les rend non prévisibles. Ainsi qu'il ressort des informations complémentaires, il convient de les limiter aux hypothèses dans lesquelles une certification obligatoire a été imposée par lesdites autorités pour des motifs de sécurité publique et de prévoir que les mesures de retrait ou de suspension du certificat d'une entité (soumise à cette certification obligatoire) seront uniquement communiquées à l'autorité désignée dans la norme qui impose cette certification obligatoire. Cela, uniquement si des mesures de publicité quant au retrait d'un tel certificat pour non-respect du schéma de certification ne sont pas prévue ; ce qu'il convient de justifier dans l'exposé des motifs.

e. En ce qui concerne les services de renseignement *: « ils ont pour mission de rechercher, d'analyser et de traiter le renseignement relatif aux menaces graves contre la sûreté de l'Etat. Lorsque cela s'avérerait nécessaire dans leurs recherches, par exemple lorsqu'une entité titulaire d'un certificat européen de cybersécurité aurait des liens avec des activités d'espionnage ou liées à une organisation criminelle, les services de renseignements devraient pouvoir avoir accès (en vertu de l'art. 14, al. 2 et art. 20, § 1er de la loi du 30 novembre 1998 sur les services de renseignement) aux informations collectées par le service d'inspection de l'autorité nationale de certification dans le cadre de ses missions de contrôle, au regard de l'importance de l'intérêt général protégé. En outre, dans la cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services. Faut encore qu'elles disposent de pouvoir d'investigation à ce sujet. »*

A ce sujet, en plus des considérations précédentes relatives aux mesures de publicité des retrait et suspension des certificats et à l'instar de la remarque faite en ce qui concerne les autorités judiciaires, l'Autorité considère qu'il n'est pas nécessaire, voir contre-productif

en terme de protection des données à caractère personnel, de répéter une communication de données au profit des services de renseignements qui est déjà encadrée par leur propre loi organique. De plus, cela sort du champ d'application de l'avant-projet de loi. Par conséquent, cet échange sera également supprimé.

f. En ce qui concerne les services de police : *« pour les mêmes motifs que ceux prévus pour les services de sécurité publique et les autorités judiciaires ».*

L'Autorité renvoie à ses remarques précitées faites à ce sujet.

13. Par conséquent, il convient de revoir le libellé des dispositions de l'avant-projet qui prévoient ces échanges (art. 6 §1 et 3, 7, 16 §2, 17 §1 et 3, 36, §1 et 3, 4° et 38) pour les rendre conformes aux considérations qui précèdent en les limitant à ce que requiert la réalisation des objectifs du Règlement cybersécurité ou de missions de services publics connexes touchant directement à la cybersécurité telles que celles poursuivies par les autorités de contrôle visées par la loi NIS (autorités sectorielles). L'auteur de l'avant-projet de loi veillera à ne pas prévoir des communications de données à caractère personnel qui sont déjà prévues par d'autres dispositions légales.

14. De plus, afin de préserver les droits et libertés des personnes physiques, clientes des prestataires contrôlés, potentiellement impactées par ces échanges, il est impératif d'insérer dans l'avant-projet de loi une disposition prévoyant que ces échanges ne peuvent pas porter sur des données à caractère personnel des clients personnes physiques (ou des clients personnes physiques de ces derniers) des prestataires de services ICT contrôlés au vu des risques importants que cela représente pour ces personnes concernées et étant donné qu'il ne ressort pas des justifications avancées par le délégué du Ministre que ces informations soient en l'espèce pertinentes et nécessaires.

15.

Enfin, au vu des objectifs du Règlement européen Cybersécurité, il importe que l'avant-projet de loi impose de manière explicite à l'Autorité nationale de certification de cybersécurité qui sera en charge du retrait des certificats une obligation d'information relative aux retraits de certificats intervenus. A cette fin, il convient d'imposer à cette Autorité de disposer d'un site web public et d'un service d'information (push) qui notifie à tous les acteurs concernés tout retrait de certification. Cela ne nécessite pas de communiquer des données à caractère personnel et cela cadre avec un des objectifs du Règlement européen Cybersécurité qui consiste à assurer la confiance dans les produits, services et processus TIC certifiés. Le cas échéant, une exception à cette publicité pourrait être envisagée pour des produits ou services TIC dont l'utilisation

nécessitent de disposer d'une habilitation de sécurité. D'un point de vue général, toute exception à la publicité des informations sur la révocation ou l'émission de certificats doit être prévue explicitement par l'avant-projet de loi et être dûment motivée et justifiée dans l'exposé des motifs.

Observations particulières

Champ d'application de l'avant-projet de loi

16. L'article 3 de l'avant-projet de loi détermine son champ d'application en précisant que la loi en projet s'appliquera à la certification européenne volontaire de cybersécurité des produits TIC, services TIC et processus TIC visée par le Règlement cybersécurité et que seuls les chapitres 1 à 4 et 7 et les articles 21 et 22 de cette loi en projet s'appliqueront aux certifications obligatoires.

17. Ainsi qu'il ressort des informations complémentaires, « *les mesures de contrôle et de sanctions liées aux certifications rendues obligatoires sont réglées ou devront être réglées par les différentes législations sectorielles applicables* ». Interrogé quant à la raison pour laquelle le chapitre 8 traitant des traitements de données à caractère personnel réalisés en exécution de la loi en projet avait été exclu des certifications européennes de cybersécurité obligatoires, le délégué du Ministre a précisé qu'il s'agissait d'un oubli et que ce chapitre 8 pouvait être inclus à l'article 3, §2 en projet. Il en est pris acte.

Désignation des autorités de contrôle compétentes

18. En exécution de l'article 58 du Règlement cybersécurité, l'article 5 de l'avant-projet de loi délègue au Roi le soin de désigner l'autorité nationale de certification de cybersécurité qui sera chargée des missions de contrôle et de supervision, visées à l'article 58 de ce Règlement. Le second paragraphe de cette disposition prévoit, à titre dérogatoire, que le Roi peut, « *en fonction du schéma de certification et à la demande de l'autorité publique concernée* », confier les missions de contrôle et de sanction (à l'exception du retrait et de la suspension des certificats) à une autre autorité publique. Interrogé à ce sujet, le délégué du Ministre a précisé que « *concrètement, il est envisagé d'utiliser éventuellement ce mécanisme au profit de l'IBPT, la FSMA, la BNB et l'inspection économique. Les dispositions modificatives ont été insérées dans le projet de loi à la demande de ces autorités car ces dernières considéraient les dispositions modificatives comme nécessaires pour que le Roi puisse éventuellement, dans les conditions imposées par la loi, les désigner*. »[8] Il en est pris acte.

[8] Au vu des désignation déjà effectuées par le biais des dispositions modificatives, l'Autorité s'interroge quant la nécessité de ces article 5, §2 en projet. Il est recommandé à l'auteur de l'avant-projet de loi de clarifier cela dans son avant-projet de loi. Dans la suite du projet d'avis, il sera référé à ces autorités de manière indifférenciée par la formulation « autorités désignées en exécution de l'article 5, §2 de l'avant-projet de loi ».

Coopération au niveau national (art. 6)

19. L'article 6 de l'avant-projet de loi traite des coopérations et échanges de données au niveau national que l'autorité nationale de certification de cybersécurité et les autorités publiques qui seront désignées en exécution de l'article 5, §2 en projet (pour l'exercice des missions visées aux chapitres 5 et 6 de l'avant- projet de loi) ainsi que d'autres autorités publiques réaliseront pour l'application du Règlement cybersécurité et de n'importe quelle autre disposition légale.

20. A ce sujet, il est renvoyé aux commentaires repris dans les observations générales du présent avis.

21. Si des collectes structurelles de données à caractère personnel doivent être réalisées par l'Autorité nationale de certification de cybersécurité et les autorités visées à l'article 5, §2 auprès de ces autorités sectorielles pour l'exercice des missions de service public prévues par le Règlement cybersécurité, elles doivent également être prévues dans l'avant-projet de loi et répondre aux mêmes critères de prévisibilité ; ce qui n'apparait pas être le cas actuellement.

22. Quant à l'article 6 § 2 en projet qui soumet les titulaires de certificat européens de cybersécurité et les émetteurs de déclaration de conformité à une obligation de communication, aux autorités en charge du contrôle du respect du règlement de cybersécurité et des schémas de certification européen, de toute information dont elles ont besoin dans l'exécution de leurs tâches, cette disposition en projet apparait redondante avec les dispositions de l'avant-projet de loi qui encadrent les pouvoirs d'inspection des services d'inspection de ces autorités et doit à ce titre être supprimée de cette partie de l'avant-projet de loi.

Echanges de données protégées par le secret professionnel ou par un devoir de confidentialité (art. 6, §4)

23. L'article 6, §4 en projet traite de la question des données protégées par le secret professionnel qui se posera dans le cadre des échanges de données que l'autorité nationale de certification de cybersécurité et les autorités visées à l'article 5, §2 en projet auront avec des tiers en ces termes :
« § 4. Les personnes dépositaires, par état ou par profession, des secrets ou informations confidentielles qu'on leur confie sont autorisées à faire connaître ces secrets ou ces informations confidentielles à l'autorité visée à l'article 5, § 1er, ainsi qu'éventuellement à d'autres autorités publiques lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.
Il s'agit notamment des informations nécessaires en matière de délivrance de certificats, de contrôle, de sanction et de réclamation. Lorsque ces informations portent sur des données à caractère personnel, le chapitre 8 est d'application. Les modalités d'échange d'informations préservent la confidentialité des informations concernées. »

24. Tout d'abord, l'Autorité ne perçoit pas en quoi la délivrance de certificats de sécurité nécessite de collecter des informations couvertes par le secret professionnel ou par un devoir de confidentialité. Selon l'exposé des motifs, seule la mission de contrôle est visée comme impactant potentiellement le secret professionnel et aucune justification quant à l'impact de la mission de délivrance de certificats de sécurité sur le secret professionnel ne ressort des informations complémentaires obtenues du délégué du Ministre. Par conséquent, à défaut de justification pertinente à ce sujet dans l'exposé des motifs, les termes « *délivrance de certificats* » seront omis de l'article 6, §4, al. 2.

25. Ensuite, l'Autorité relève qu'il y a, en matière d'échange de données protégées par le secret professionnel ou par un devoir de confidentialité, deux cas de figure qu'il convient de distinguer :
    a. tout d'abord, la situation dans laquelle se trouve une autorité soumise à un devoir de confidentialité qui se voit empêchée de communiquer des informations couvertes par ce devoir de confidentialité alors que lesdites communications sont légitimes, pertinentes et nécessaires (cf. supra) ;
    b. ensuite, la collecte, par les services d'inspection des autorités en charge du contrôle du respect du Règlement cybersécurité, de données à caractère personnel protégées par le secret professionnel (par exemple lors d'audit de systèmes ICT certifiés).

26. Ces deux situations doivent être appréhendées de manière distincte par l'avant-projet de loi et seule la première doit être abordée dans l'article 6 au vu de son intitulé (« *coopération au niveau national* »).

27. La disposition légale appréhendant le premier cas de figure (23.a) doit être de rédigée de manière telle que la levée de confidentialité ne peut avoir lieu qu'au profit d'autorités pour lesquelles les échanges de données sont légitimes[9], pertinents et nécessaires (cf. supra) pour l'exercice des devoirs d'inspection des autorités visées à l'article 5 de l'avant-projet de loi. De plus, le terme « *notamment* » à l'alinéa 2 du §4 de l'article 6 en projet doit être supprimé pour limiter correctement l'objet desdits échanges.

28. Quant au second cas de figure d'échange de données impactant le secret professionnel, c'est sous le chapitre traitant des pouvoirs d'inspection qu'il doit être appréhendé. Des garanties spécifiques pour les droits et libertés des personnes concernées par les données couvertes par ce secret professionnel doivent impérativement être prévues par l'avant-projet de loi de manière claire si et seulement si l'accès à de telles données est indispensable pour la réalisation des mesures

[9] En faisant référence à la disposition de l'avant-projet de loi qui décrira les modalités de ces échanges conformément aux observations de l'Autorité (cf. supra).

d'investigation du service d'inspection (autorisation préalable du juge d'instruction, intervention de l'Ordre professionnel auquel appartient la personne dont les documents devront être consultés pour la réalisation des contrôles précités sous peine de mettre en péril lesdits contrôles, interdiction de conservation de documents couverts par le secret professionnel par les autorités précitées,…cf. à ce sujet les articles 56bis et 90 octies du Code d'instruction criminelle). A défaut, il sera alors explicitement prévu que toute information couverte par le secret professionnel au sens de l'article 458 du Code pénal ne peut pas être collectée par le service d'inspection.

Chapitre 5 – Contrôle (art. 13 à 18)

29. Les articles 13 à 18 de l'avant-projet de loi encadrent la procédure de contrôle de l'autorité nationale de certification de cybersécurité et les pouvoirs dont disposera son service d'inspection.

30. L'article 13, §2 de l'avant-projet formalise les demandes d'informations que les inspecteurs pourront réaliser dans le cadre de leur mission, en ces termes :
« *Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande et précise le délai dans lequel les informations ou preuves doivent être fournies.* »

31. Afin que la personne contrôlée soit à même d'apprécier la pertinence et le caractère nécessaire des données (le cas échéant à caractère personnel) qui seront nécessaires dans ce cadre, il convient que cette disposition prévoie explicitement que les inspecteurs devront identifier les dispositions légales ou la ou les parties du schéma de certification auxquelles une infraction est suspectée.

Pouvoirs de contrôle du service d'inspection de l'autorité nationale de certification de cybersécurité – Mise en place de garanties pour la protection des données à caractère personnel reprises dans les systèmes informatiques audités

32. Les larges pouvoirs de contrôle du service d'inspection de l'autorité nationale de certification de cybersécurité sont décrits à l'article 15 de l'avant-projet de loi.

33. A l'instar de ce qui est prévu pour les perquisitions à l'article 15, §4 en projet, l'Autorité recommande d'ajouter dans l'avant-projet de loi des garde-fous pour les pouvoirs qui sont particulièrement intrusifs et qui permettront au service d'inspection d'avoir accès aux données à caractère personnel des clients (ou de la clientèle de ces derniers) des prestataires de services TIC ou fournisseurs de produits TIC qui seront contrôlés. A cet effet, au titre de garanties pour la préservation des droits et libertés des personnes concernées, il convient notamment d'interdire explicitement au service d'inspection de collecter ou de communiquer les données des clients (ou

de la clientèle de ces derniers) des prestataires et fournisseurs contrôlés pour des finalités autres que le contrôle du respect du règlement ou du schéma de certification concerné. Au même titre, l'Autorité considère qu'il convient de prévoir, à l'instar de ce qui est prévu à l'article 66 de la loi précitée du 7 avril 2019 (loi NIS), que, dès que des données à caractère personnel autres que celles concernant le titulaire du certificat européen ou les membres de son personnel doivent être accédées pour la réalisation des contrôles du service d'inspection, ces données doivent être, si possible, préalablement pseudonymisées selon les règles actuelles de l'art[10].

34. L'Autorité recommande également que le respect du principe de proportionnalité dans l'exercice des pouvoirs d'investigation soit explicitement inscrit dans l'avant-projet de loi, à l'instar de ce qui est fait pour d'autres pouvoirs d'inspection tels que ceux de l'inspection sociale (cf. code pénal social). Ainsi, il sera explicitement prévu, à l'article 15 de l'avant-projet de loi, que « lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les inspecteurs de l'autorité nationale de certification de cybersécurité et des autorités visées à l'article 5, §2 en projet veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour le contrôle du Règlement cybersécurité ou des dispositions du schéma de certification dont ils contrôlent le respect ». Les collectes de données à caractère personnel qu'ils réalisent dans l'exercice de leurs missions de contrôle doivent se limiter aux seules données pertinentes pour prouver une infraction au règlement cybersécurité ou le non-respect d'un schéma de certification. Ils ne disposent d'ailleurs dans ce cadre pas d'autres pouvoirs que ceux-là.

35. Enfin, l'Autorité rappelle que l'opportunité de mener des investigations s'appréciera, dans le chef des inspecteurs, *in concreto,* au regard des éléments de fait à leur disposition. Ils disposent d'un pouvoir d'appréciation dans ce cadre. Les inspecteurs réaliseront les collectes électroniques de données nécessaires avec discernement et modération et n'accèderont à des données à caractère personnel que si, à la lumière des faits, ils disposent d'un faisceau d'indices concordants et sérieux que les données à caractère personnel recherchées rendraient possible ou accéléraient la prévention et la détection des infractions au Règlement cybersécurité ou au schéma de certification dont le respect est contrôlé.

Communication par le service d'inspection de ses rapports d'inspection et PV de contrôle à des tiers

36. L'article 16, §2 de l'avant-projet de loi prévoit que l'autorité nationale de certification de cybersécurité ou l'autorité désignée par le Roi en vertu de l'article 5, §2 de l'avant-projet de loi

[10] Cf à ce sujet ENISA : https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases et https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation;

communique une copie de son rapport d'inspection aux « *autorités de surveillance de marché, à l'autorité nationale d'accréditation, aux services de sécurité publique, aux services de police, au services de renseignement et à l'autorité visée à l'article 7,§4 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, à leur demande et pour autant que cela poursuive l'accomplissement de leurs missions légales*».

37. Pour les motifs évoqués sous les observations générales du présent avis, l'Autorité ne perçoit pas en quoi une telle communication sur simple demande s'avère opportune pour les services de renseignement, de sécurité publique et les services de police pour la bonne exécution du Règlement cybersécurité. Interrogé à ce sujet, le délégué du Ministre a précisé que « *la transmission d'une copie d'un rapport d'inspection ou d'un procès-verbal relatif au contrôle d'un certificat de cybersécurité par l'une des autorités précitées peut s'avérer nécessaire à l'exécution des missions légales de ces autorités ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique* » et a cité des dispositions légales existantes permettant à certaines autorités comme le Centre de crise nationale ou l'OCAM de disposer d'information de ce type. A ce sujet, l'Autorité relève tout d'abord que l'auteur de l'avant-projet de loi doit veiller à ne pas prévoir, en des termes flous, des flux de donnée qui sont déjà encadrés par d'autres dispositions légales. De plus, il ne rentre dans les objectifs de l'avant-projet de loi ni dans son champ d'application d'encadrer les pouvoirs d'inspection d'autres autorités publiques que celles qui sont chargées du contrôle du respect du règlement européen et des schémas de certification adopté en exécution dudit règlement. Ensuite, afin d'assurer la proportionnalité de cette disposition en projet, il convient de déterminer clairement dans l'avant-projet de loi les circonstances et finalités, légitimes et pertinentes pour l'exécution du Règlement européen cybersécurité, dans lesquelles lesdits rapports peuvent être communiqués aux seules autorités qui disposent de missions de service public spécifique en matière de cybersécurité et ce, en lieu et place de prévoir des communications sur simple demande sans autre précision et ce sans préjudice d'autres dispositions légales permettant à des autorités publiques d'accéder à certains rapport ou à certaines informations y reprises.

38. De plus, à l'instar de ce qui a déjà été recommandé, il convient de préciser que ces rapports ne peuvent contenir des données à caractère personnel concernant des clients (ou la clientèle de ces derniers) des prestataires de services ICT contrôlés au vu des risques que cela représente pour ces personnes concernées. Pour le surplus, l'Autorité renvoie à ses considérations générales reprises ci-dessus. Le libellé de l'article 16, §2 en projet devra être revu en conséquence.

39. L'article 16, §3 en projet détermine les destinataires auxquels ces rapports d'inspection devront être systématiquement transmis en cas de *« contrôle effectué auprès d'une infrastructure critique,*

d'un opérateurs de service essentiel ou d'un fournisseur de service numérique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien ».

40. Ce faisant, l'avant-projet de loi instaure une obligation légale de traitement de données à caractère personnel (dans l'hypothèse où ces rapports contiendront des données à caractère personnel ou porteront sur un prestataire/fournisseur de service/produit ICT exerçant en personne physique) au sens de l'article 6.1.c du RGPD. Etant donné que les législations spécifiques visées à l'article 16, §3 en projet poursuivent un objectif similaire à celui du Règlement cybersécurité, l'Autorité n'a pas d'objection aux communications des rapports dans l'hypothèse où une inspection des autorités visées à l'article 5 de l'avant-projet de loi portent sur des entités utilisant lesdits services ou produits ICT visés par les législations mentionnées à l'article 16, §3. Par souci de sécurité juridique et de prévisibilité et par souci de conformité avec l'article 6.3 du RGPD, il convient toutefois de définir adéquatement la notion « *d'autorité sectorielle et de service d'inspection compétents* », de déterminer, à l'article 16, §3, la finalité précise pour laquelle ces rapports seront utilisés par ces autorités destinataires (à savoir, l'exercice de leurs missions de service public conférées par lesdites réglementations spécifiques) et de préciser que les rapports doivent être adressés uniquement à l'autorité sectorielle compétente en fonction du prestataire ou fournisseur de service ICT concerné par le rapport.

41. L'article 17 §1 à 4 de l'avant-projet détermine de manière très large la communication à des tiers de données et procès-verbaux de contrôle par le service d'inspection de l'autorité nationale de certification.

42. Le « *besoin d'en connaître en raison des missions poursuivies en lien avec la présente loi ou d'autres dispositions légales* » prévu à l'article 17, §1 en projet est un critère flou et trop large pour encadrer la communication de données à caractère personnel collectées par le service d'inspection à d'autres autorités d'autant plus que le §2 de cet article 17 en projet soumet le service d'inspection au secret professionnel. Par conséquent, cet article 17, §1 sera supprimé.

43. Quant à l'article 17, §3 en projet qui prévoit la communication par le service d'inspection de tout PV ou information complémentaire aux diverses autorités visées, l'Autorité renvoie aux remarques émises en observations générales dans le présent avis ainsi qu'aux remarques émises sur l'article 16, §2 en projet qui s'appliquent *mutatis mutandis.* De même, pour l'article 17, §4, il est renvoyé aux remarques émises sur l'article 16, §3.

Dérogation au principe de confidentialité des communications électroniques au profit du service d'inspection de l'autorité nationale de certification de cybersécurité

44. L'article 17, §5 en projet prévoit, en ces termes, une dérogation au principe de confidentialité des communications effectuées au moyen d'un réseau public et d'un service de communications électroniques accessibles au public[11] au profit du service d'inspection de l'autorité nationale de certification de cybersécurité:

« §. 5. Dans l'exercice de leurs fonctions, les membres du personnel du service d'inspection peuvent :
1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne leur est pas destinée personnellement ;
2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;
3° prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne. »

45. C'est dans les limites prévues à l'article 15 de la Directive ePrivacy que telles dérogations peuvent être prévues. L'article 15.1 de la Directive ePrivacy prévoit que : «*les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, […] et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne* »[12]. Avec l'entrée en vigueur du RGPD, il convient de lire l'article 15 de la Directive ePrivacy comme faisant référence à l'article 23 du RGPD. Cette disposition du RGPD prévoit notamment comme motif de limitation aux droits des personnes concernées « *l'exercice d'une mission de contrôle, d'inspection ou de réglementation liées, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a), b), c), d), e) et g)* » ; à savoir, notamment, la sécurité et la défense nationale, la sécurité publique, la prévention et détection d'infraction

[11] consacré par l'article 5.1 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 (dite « Directive ePrivacy) implémenté en droit belge à l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques

[12] L'article 6 §§ 1 et 2 du traité sur l'Union européenne se lit comme suit : « 1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités […]. Il ressort de la jurisprudence de la CJUE que tous les causes de justification prévues à l'article 23 (ex 13 de la directive 95/46) du RGPD peuvent justifier une dérogation à ce principe de confidentialité des communications électroniques.

pénale, d'autres objectifs importants d'intérêts public général notamment un intérêt économique ou financier important et la prévention et détection de manquements à la déontologie de profession réglementée.

46. Il appartient tout d'abord à l'auteur de l'avant-projet de loi d'expliciter dans l'exposé des motifs en quoi la dérogation envisagée au profit du service d'inspection de l'autorité nationale de certification de cybersécurité cadre avec un ou plusieurs des motifs explicités à l'article 23.1 du RGPD.

47. Ensuite, au vu des motifs sur base desquels une dérogation à ce principe de confidentialité peut être prévue par les Etats membres, l'Autorité s'interroge s'il ne conviendrait pas en l'espèce de limiter ces dérogations aux contrôles qui seront opérés sur les organismes d'évaluation de la conformité ainsi que sur les titulaires de certificats obligatoires étant donné que c'est dans des domaines d'intérêt public important que des mesures législatives devraient être adoptées pour imposer de tels certificats. Il est indiqué que l'auteur de l'avant-projet de loi justifie sous cet angle le choix qu'il posera pour le champ d'application de la dérogation et insère sa justification dans l'exposé des motifs.

48. Interrogé quant aux besoins du service d'inspection nécessitant la mise en place d'une telle dérogation au principe de confidentialité des communications électroniques, le délégué du Ministre a précisé que « *ne sont pas visées les écoutes téléphoniques mais la* (prise de connaissance) *des e-mails émanant et reçus des organismes d'évaluation de la conformité, des émetteurs de déclaration de conformité, des titulaires de certificat de cybersécurité européen et ce uniquement lorsque les données en question sont susceptibles de contribuer à l'élucidation d'un manquement grave à un schéma de certification dont le respect est contrôlé* ».

49. Par conséquent, afin de garantir le caractère proportionné de la dérogation, il appartient à l'auteur de l'avant-projet de loi de préciser, à l'article 17, §3 en projet, que c'est uniquement les communications électroniques émanant et reçues des organismes d'évaluation de la conformité, (des émetteurs de déclaration de conformité)[13], des titulaires de certificat (obligatoire)[14] de cybersécurité européen que les inspecteurs pourront prendre connaissance et ce, uniquement si ces informations sont susceptibles de contribuer à l'élucidation d'un manquement grave à un schéma de certification (obligatoire) contrôlé ou au Règlement européen cybersécurité. Par souci de sécurité juridique et de prévisibilité, il sera aussi explicitement précisé que l'article 17, §3 déroge à l'article 124 de la loi précitée du 13 juin 2005.

[13] En fonction du choix qui devra être opéré au regard de la considération précédente.

[14] *Ibidem*

50. Enfin, interrogé quant à l'opportunité de prévoir des garanties pour les personnes contrôlées tel que leur accord préalable pour la consultation de leur communications électronique ou à défaut, l'accord du juge d'instruction, le délégué du Ministre a précisé que « *en l'absence du consentement expresse de l'entité contrôlée, les membres assermentés du service d'inspection de l'autorité nationale de certification de cybersécurité ne pourront pas prendre connaissance de ces informations (ceux-ci n'ayant pas la qualité d'officier de police judiciaire) ».* Il est donc indiqué de prévoir à l'article 17, §3 en projet que c'est après accord de la personne contrôlée que les consultations visées auront lieu.

Chapitre 8 – Traitement de données à caractère personnel

51. L'auteur de l'avant-projet de loi a opté pour l'insertion d'un chapitre spécifique dans son avant-projet visant à déterminer différents éléments des traitements de données à caractère personnel encadrés par l'avant-projet de loi.

Catégories de traitement de données à caractère personnel et finalités desdits traitements

52. L'article 36, §1er et 3 décrit les catégories de traitements de données à caractère personnel réalisés dans le cadre de l'exécution de la loi en projet en ces termes :

« *Art. 36. § 1er. Les traitements de données à caractère personnel effectués dans le cadre de l'exécution de la présente loi sont les suivants :*

1° l'échange d'informations entre l'autorité visée à l'article 5, § 1er, l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, les autorités judiciaires, les autorités sectorielles ou les services d'inspection visés respectivement à l'article 7, § 3 et § 5 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les autorités de surveillance de marché, l'autorité nationale d'accréditation, les services de sécurité publique, les services de police, les services de renseignement et l'autorité visée à l'article 7, § 4 de la du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

(…)

2° l'échange d'informations entre les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne, d'une part, et l'autorité visée à l'article 5, § 1er ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, d'autre part.

(…)

3° le traitement de données par l'autorité visée à l'article 5, § 1er ou par un organisme d'évaluation de la conformité, pour accomplir les tâches en matière de réclamation visées au chapitre 7.

(…) ;

4° le traitement de données par l'autorité visée à l'article 5, § 1er ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, relatives à ses tâches en matière de contrôle et de sanction.
(…)
§ 3. Les finalités pour lesquelles les traitements visés au paragraphe 1er sont effectués, sont les suivantes :
1° la délivrance de certificats de cybersécurité européens ;
2° la supervision des titulaires de certificats de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne ou des organismes d'évaluation de la conformité ;
3° le traitement des réclamations introduites sur base de l'article 63, § 1er du Règlement sur la cybersécurité ;
4° la coopération, en ce compris l'échange d'informations, au niveau national et international ;
5° l'imposition des sanctions prévues au chapitre 6. »

53. Tout d'abord, l'Autorité relève que la notion de « *traitements de données à caractère personnel effectués dans le cadre de l'exécution de la présente loi* » ne sert pas les exigences de prévisibilité. Au vu du champ d'application de l'avant-projet de loi, il convient d'encadrer uniquement les traitements de données à caractère personnel que réaliseront l'autorité nationale de certification de cybersécurité ainsi que le cas échéant les autorités désignées en exécution de l'article 5,§2 de l'avant-projet de loi (pour autant que ces derniers traitements ne sont pas déjà encadrés par les lois organiques de ces autorités) en exécution des missions de service public décrites au Règlement européen cybersécurité et que la loi en projet leur octroie. L'avant-projet de loi ne doit pas encadrer des traitements de données qui sortent de ce champ d'application ou qui sont par ailleurs déjà encadrés par les lois organiques d'autres autorités ; ce qu'il appartient à l'auteur de l'avant-projet de loi de vérifier.

54. Une description exhaustive des catégories de traitements de données réalisés en exécution de la loi en projet, tel que tente de le faire l'article 36, §1 en projet, risque de porter préjudice à l'exercice des missions de service public de l'autorité nationale de certification dans l'hypothèse où interviendrait un oubli. Une détermination claire et concrète des finalités des traitements de cette autorité (en plus de la détermination de leurs autres éléments essentiels) doit suffire à assurer la prévisibilité requise à ces traitements de données à caractère personnel. L'Autorité recommande la suppression de l'article 36, §1 en projet.

55. Quant à la détermination des finalités des traitements, faite à l'article 36, §3 en projet, il convient de viser les finalités pour lesquelles l'autorité nationale de certification et/ou les autorités qui seront désignés en exécution de l'article 5, §2 de l'avant-projet de loi traiteront des données à caractère personnel dans le cadre des missions de service public qui leur sont octroyées par

l'avant-projet de loi et le Règlement européen cybersécurité[15]. Les remarques suivantes s'imposent à ce sujet :

a. Les finalités visées à l'article 36, §3, 1° et 3° seront utilement fusionnées : délivrance des certificats de cybersécurité européen et gestion des réclamations y relatives ;
b. Les finalités visées à l'article 36, § 3, 2° et 5° seront également fusionnées et il sera fait référence aux dispositions pertinentes de l'avant-projet de loi en ces termes : contrôle des titulaires de certificat de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne et des organismes d'évaluation de conformité et le cas échéant imposition de sanction conformément aux chapitres 5 et 6 de la présente loi ;
c. Quant à la « coopération, en ce compris l'échange d'information au niveau national et international », il ne s'agit pas d'une finalité de traitement au sens du RGPD mais d'un traitement de données en soi qui doit être déjà couvert par les finalités de contrôle et de sanction précitées voir, si nécessaire et conforme au Règlement cybersécurité, par la finalité de « *délivrance des certificats* ». L'article 36, §3, 4° sera par conséquent supprimé et le cas échéant, si les dispositions législatives existantes (Loi NIS) ne prévoient pas déjà de manière prévisible lesdits flux, cette disposition en projet sera remplacée par la finalité concrète pour laquelle une communication d'informations sera réalisée par l'autorité nationale de certification et les autorités désignées en exécution de l'article 5, §2 en projet aux seules autorités sectorielles compétentes (NIS) et ce, conformément aux articles 16 et 17 de l'avant-projet de loi (adaptés conformément aux recommandations précitées de l'Autorité). De plus, si l'auteur de l'avant-projet de loi vise la participation de l'Autorité nationale de certification de cybersécurité à la coopération internationale en vue de l'amélioration de la qualité des certifications et l'harmonisation des approches en la matière et qu'une telle coopération nécessite un échange de données à caractère personnel entre les autorités nationales de certification de cybersécurité, il est indiqué de mentionner une telle finalité de manière concrète et précise.

Qualification du responsable du traitement

56. Afin d'éviter toute ambiguïté quant à l'identité de l'entité qui doit être considérée comme responsable du traitement et afin de faciliter ainsi l'exercice des droits de la personne concernée tels que prévus aux articles 12 à 22 du RGPD, l'Autorité invite l'auteur de l'avant-projet de loi à identifier plus explicitement que ce qu'il ne fait à l'article 36, §1 en projet le ou les responsables de traitement.

[15] L'article 36 en projet vise actuellement l'encadrement des « *traitements de données réalisé en exécution de la loi* » Or, tous les traitements de données réalisés pour la finalité de « *délivrance des certificats de cybersécurité européens* » ne sont, à juste titre, par couverts par l'avant-projet de loi. Le libellé de l'article 36 en projet sera donc revu sur ce point.

57. A cet effet, la précision selon laquelle l'autorité nationale de certification de cybersécurité est responsable des traitements qu'elles réalisent pour la réalisation des finalités visées à l'article 36, §3 suffit. Il en sera fait de même pour les autorités visées à l'article 5, §2 de l'avant-projet en ce qui concerne les traitements réalisés pour les finalités de contrôle et de sanction visées au chapitre 5 et 6 de l'avant-projet de loi.

Base de licéité

58. L'article 36, §2 en projet la base de licéité des traitements visés en ces termes
« § 2. Les traitements visés au paragraphe 1er sont nécessaires pour respecter les obligations légales découlant du Règlement sur la Cybersécurité ou de la présente loi, ou exécuter une mission d'intérêt public dont est investi l'une des autorités publiques visées par la présente loi. »

59. L'Autorité relève que la majorité des traitements de données à caractère personnel visés par la loi en projet seront des traitement réalisés par l'autorité nationale de certification de cybersécurité (et les autorités visées à l'article 5, §2 en projet) en exécution de ses missions de service public ; dont la base de licéité, au sens du RGPD, est l'article 6.1.e du RGPD (à l'exception des communications obligatoires systématiques de rapports et procès-verbaux d'inspection prévues aux articles 16, §3 et 17§4 de l'avant-projet de loi, dont la base de licéité est l'article 6.1.c du RGPD).

60. L'article 36, §2 en projet n'apporte aucune plus-value en termes de prévisibilité des traitements de données visés. Pour assurer la licéité et la prévisibilité des traitements qui se fondent sur l'article 6.1.e. du RGPD, une norme juridique nationale ou supranationale d'application directe doit déterminer de manière suffisamment claire et précise les missions de service public dont est investi le responsable du traitement (ce qui est le cas dans l'avant-projet de loi et le Règlement européen cybersécurité), mais il n'est pas requis que cette norme ou la norme nationale d'exécution d'un Règlement européen précise que les traitements de données effectués à cette fin le sont en «*exécution d'une mission d'intérêt public dont est investi le responsable du traitement* ». En conséquence, cet article 36, §2 en projet sera supprimé.

Catégories de données à caractère personnel traitées

61. L'article 36, §4 détermine, en ces termes, les catégories de données à caractère personnel traitées :
« § 4. Les données personnelles traitées sont des données d'identification ou d'authentification et des données de communications électroniques.

Le Roi peut, après avis de l'autorité visée à l'article 5, § 1er ou de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, compléter l'alinéa précédent par d'autres données à caractère personnel. »

62. Outre le fait que l'avant-projet de loi ne précise pas par quelle entité ces catégories de données sont traitées, cette détermination ne présente pas de plus-value en termes de prévisibilité des traitements de données visés. De plus, en application du principe de légalité, l'Autorité considère qu'il ne peut en l'espèce être délégué au Roi le soin de compléter la liste des catégories de données à caractère personnel qui devront être traitées par l'Autorité nationale de certification de cybersécurité et les autorités désignées en application de l'article 5, §2 de l'avant-projet de loi pour la réalisation des missions de service public que l'avant-projet de loi leur confie. La liste actuelle étant manifestement lacunaire (quid des données relative à l'expertise ou à la formation du personnel du prestataire certifié ou en cours de certification ?...), il convient de la compléter au regard des critères communs (common criteria)[16] en la matière et son contenu doit être dûment justifié et motivé dans l'exposé des motifs.

63. En ce qui concerne les catégories de données traitées en application des chapitres 5 et 6 de l'avant-projet de loi (contrôle et sanction), l'Autorité reconnait qu'l n'est pas envisageable de les déterminer autrement que de manière fonctionnelle, en précisant qu'il s'agit des données nécessaires à l'exercice des missions de contrôle et de sanction visées aux chapitre 5 et 6 de l'avant-projet..

64. Par conséquent, l'article 36, §4 de l'avant-projet de loi sera revu en conséquence.

Catégories de personnes physiques à propos desquelles des données sont traitées

65. L'article 36 §5 détermine, en ces termes, les catégories de personnes à propos desquelles des données sont traitées pour la réalisation des finalités précitées :
« § 5. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet des traitements visés au paragraphe 1er sont les suivantes :
1° toute personne intervenant pour les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne ou une autorité publique ;

[16] Les Critères communs d'évaluation de la sécurité des technologies de l'information (appelés Critères communs ou CC) sont une norme internationale (ISO/IEC 15408) pour la certification de la sécurité informatique.

2° toute personne participant à un contrôle ou à une audition dans le cadre des missions de contrôle prévues au chapitre 5 ;
3° toute personne introduisant une réclamation. »

66. Tout d'abord, il convient de viser les personnes physiques et non simplement les personnes.

67. Ensuite, l'Autorité s'interroge quant au caractère éventuellement lacunaire de cette énumération au vu de ses observations générales reprises en début d'avis. Si tel est le cas, il convient d'y pallier et, au titre de garantie pour la préservation des droits et libertés des clients (ou de la clientèle de ces derniers) des prestataires des services/fournisseurs de produits ICT et conformément aux considérations générales de l'Autorité reprises en début d'avis, il importe de préciser que l'autorité nationale de certification de cybersécurité et les autorités désignées en application de l'article 5, §2 en projet, ne peuvent traiter des données concernant des personnes physiques clientes (ou la clientèle de ces dernières) des prestataires de services/fournisseurs de produits ICT contrôlés pour des finalités autres que le contrôle du respect par ces prestataires/fournisseurs du Règlement européen cybersécurité et des schémas européens de certification qui font l'objet du contrôle.

Durée de conservation

68. L'article 39 détermine la durée de conservation des données collectées en exécution de l'avant-projet de loi en ces termes :
« Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, visé à l'article 89 du Règlement UE 2016/679, les données à caractère personnel traitées en exécution de la loi sont conservées, sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 3. »

69. Comme déjà explicité ci-dessus, c'est la durée de conservation des données à caractère personnel collectées par l'autorité nationale de certification de cybersécurité et les autorités qui seront désignées en exécution de l'article 5, §2 en projet pour la réalisation des finalités visées à l'article 36, §3 qu'il convient de déterminer. La formulation de l'article 39 en projet sera utilement adaptée en ce sens.

70. En ce qui concerne la durée de conservation prévue, l'Autorité n'a pas de remarque à formuler.

Dérogation aux droits des personnes concernées

71. L'article 37 de l'avant-projet de loi déroge de manière très large à tous les droits des personnes concernées en vertu du RGPD.

72. Toute limitation aux droits dont disposent les personnes concernées en vertu du RGPD doit, non seulement, poursuivre un des objectifs énumérés à l'article 23.1 du RGPD, mais également répondre aux formes prescrites par l'article 23.2 du RGPD. De plus, toute limitation aux droits des personnes concernées se doit également d'être limitée au strict nécessaire tant en termes d'ampleur que de durée[17].

73. Tout d'abord, il convient de viser explicitement les responsables du traitement bénéficiant desdites dérogations, à savoir, ainsi qu'il ressort des informations complémentaires, l'autorité nationale de certification de cybersécurité et les autorités qui seront désignées en exécution de l'article 5, §2 en projet.

74. Selon l'article 37 en projet, les traitements desdits responsables qui bénéficieront de la dérogation envisagée sont ceux qui seront effectués pour la finalité de contrôle ainsi que pour la finalité de gestion des réclamations relatives à l'octroi d'un certificat de cybersécurité ou au refus de délivrance d'un tel certificat.

75. Bien que l'Autorité comprenne la nécessité de prévoir des dérogations à certains droits garantis par le RGPD pour les traitements de contrôle (pour ne pas mettre en péril ces opérations de contrôle), l'Autorité s'interroge quant à la nécessité de prévoir ce type de dérogation pour la gestion des réclamations relative à l'octroi ou au refus d'octroi des certificats. Pour ces derniers traitements, l'Autorité peut, par contre, comprendre la nécessité de prévoir dans l'avant-projet de loi la possibilité pour un plaignant de solliciter le traitement de sa réclamation de manière telle que son anonymat soit préservé (pour autant que la gestion de sa réclamation le permette) mais, outre cette hypothèse qui peut être prévue dans l'avant-projet de loi, il n'apparait pas nécessaire, au vu des informations complémentaires obtenues, de prévoir une dérogation au droits visés aux articles 12 à 22 du RGPD pour assurer le traitement adéquat des réclamations. A défaut de justification pertinente à ce sujet dans l'exposé des motifs, le champ d'application de la dérogation sera réduit en conséquence.

[17] Avis n° 34/2018 du 11 avril 2018 *concernant un avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre 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* et plus spécifiquement ses considérants 36 à 38 ; Avis n° 41/2018 du 23 mai 2018 *concernant un avant-projet de loi portant des dispositions financières diverses* ; Avis n° 88/2018 du 26 septembre 2018 *sur le projet d'arrêté du Gouvernement flamand portant adaptation des arrêtés du Gouvernement flamand au règlement (UE).*

76. Ensuite, concernant la dérogation au profit des traitements de données réalisés par les services d'inspection aux fins d'exercice de leurs missions de contrôle prévue à l'article 13 de l'avant-projet de loi, l'Autorité relève que, en application de l'article 23.2 du RGPD, c'est à l'auteur de l'avant-projet de loi de préciser, à l'article 37 en projet, l'étendue des limitations introduites non seulement en terme de droits auxquels il est dérogé mais aussi en terme de limites de la dérogation prévue et ce, en lieu et place de prévoir que « *l'exemption ne vaut que si et dans la mesure où ces traitements sont nécessaires pour les finalités définies ci-avant, notamment dans la mesure où l'application des droits prévus par le règlement précité nuirait aux besoins d'un contrôle, d'une enquête ou d'une réclamation » ;* ce qui ne sert pas la sécurité juridique requise en la matière.

77. A ce sujet, sans viser à l'exhaustivité, l'Autorité recommande de préciser que les dérogations aux droits des personnes concernées ne sont d'application que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête (y compris les actes préparatoires de maximum 1 an après réception de la demande d'exercice du droit[18]) et pendant la période nécessaire en vue d'exercer les poursuites en la matière et ce, dans la mesure où l'exercice des droits nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires.

78. Quant au choix des articles du RGPD auxquels il est décidé de déroger dans l'avant-projet de loi pour l'exercice de la mission d'inspection, les remarques suivantes s'imposent :
    a. L'article 12 du RGPD explicite la transparence des informations et communication et modalités de l'exercice des droits des personnes concernées et ne constitue pas en soi un droit des personnes concernées. Il n'y a pas lieu d'y déroger.
    b. La nécessité de déroger au droit à l'effacement (art. 17 RGPD) pour l'objectif poursuivi n'apparait pas. Interrogé à ce sujet, le délégué du Ministre a précisé qu'« *il est prévu que les données à caractère personnel soient conservées sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 3. Cette durée se justifie par la nécessité de s'assurer de conserver plus longtemps les données à caractère personnel pouvant être liées à un faux ou usage de faux relatif à une certification de cybersécurité. Le service d'inspection doit également pouvoir d'identifier les cas de récidive pour les mêmes faits dans un délai de trois ans (qui peuvent donner lieu au doublement de l'amende administrative en vertu de l'article 24, § 4 de l'avant-projet). Or, sur base du droit à l'effacement, la personne concernée pourrait obtenir l'effacement prématuré de ses données. Il apparaît donc nécessaire de limiter ce droit* ». A ce sujet, l'Autorité relève que le droit à l'effacement ne permet pas à une personne concernée d'obtenir l'effacement de

[18] Afin d'assurer une limitation dans le temps raisonnable à la dérogation.

ses données de manière prématurée mais uniquement quand un des motifs visés à l'article 17 s'applique, ce qui n'apparait pas en l'espèce comme invalidant pour la procédure de contrôle du service d'inspection. Il convient d'ailleurs de relever que les services de l'inspection sociale et de l'inspection fiscale ne bénéficient pas non plus de dérogation à ce droit alors que les motivations de leurs dérogations aux droits des personnes concernées du RPGD sont les mêmes. Par conséquent, la dérogation à ce droit sera supprimée de l'article 37 en projet.

c. Dans le même ordre d'idées que ce qui précède, la dérogation au droit d'opposition sera également ôtée de l'article 37 en projet et ce, pour les mêmes motifs. L'article 21 du RPGD prévoit que lorsqu'une personne concernée s'oppose à un traitement de ses données qui est fait pour l'exercice d'une mission de service public, « *le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne prouve qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou la constatation, l'exercice ou la défense de droits en justice* » ; ce que l'autorité de certification n'aura pas de mal à prouver dans l'hypothèse où un tel droit est exercé par une personne contrôlée ; ce qui est d'ailleurs fort improbable étant donné qu'une personne concernée ne sait exercer ce droit que lorsqu'elle a connaissance d'un contrôle à son égard ; ce qui ne sera pas le cas étant donné qu'il est dérogé aux droits d'information et d'accès.

d. Quant à la dérogation à l'article 22 du RGPD faite par l'article 37 en projet, le délégué du Ministre a fait valoir à cet égard que « *des décisions individuelles automatisées (fondées sur l'utilisation d'algorithmes) en matière de contrôle et de sanctions ne sont pas prévues à ce stade mais leur utilisation pourrait s'avérer dans le futur utile ou nécessaire*. » Conformément à l'article 22.2 du RGPD, pour que les autorités visées à l'article 5 de l'avant-projet de loi puissent adopter des décisions fondées exclusivement sur un traitement automatisé produisant des effets juridiques sur la personne concernée ou l'affectant de manière significative, lesdites décisions doivent être prévues par une disposition législative spécifique qui doit encadrer lesdites décisions automatisées et prévoir des mesures appropriées pour la sauvegarde des droits et liberté et des personnes concernées ; ce qui n'est pas le cas de l'avant-projet de loi soumis pour avis. Par conséquent, la dérogation à l'article 22 du RGPD n'apparait pas nécessaire et doit également être omise.

e. Il convient également d'ôter l'article 20 du RGPD de la liste des articles auxquels il est dérogé étant donné qu'il n'est de toute façon pas d'application en l'espèce, ce qui a été confirmé par le délégué du Ministre.

79. De plus, pour rendre l'article 37 en projet compatible avec l'article 23.2 du RGPD, il convient de prévoir des garanties similaires à ce qui est prévu au chapitre 5/1 du code pénal social, lesdites dérogations et les garanties pour les droits et libertés des personnes concernées ayant déjà été approuvées par l'autorité de protection des données[19] (association du délégué à la protection des données autorités visées à l'article 5 en projet pour la consignation des motifs de fait ou de droit sur lesquels se fonde la décision de refus d'accéder au droit de la personne concernée et mise à disposition desdits motifs à l'Autorité de protection des données à 1ère demande, information des personnes concernées du refus d'accéder à sa demande et des motifs sauf si cela risque de compromettre la finalité de contrôle, information des personnes concernées ayant souhaité exercer leurs droits de la levée de la dérogation dès la clôture du contrôle, information des personnes concernées des recours dont elles disposent dans ce cadre, …).

80. L'Autorité ne perçoit pas la pertinence de l'article 37, §4 en projet. Il ne sert par ailleurs pas la sécurité juridique requise en matière de dérogation à un droit fondamental. Sa suppression est recommandée.

81. L'article 37, §5 sera également supprimé étant donné qu'il est redondant par rapport à d'autres dispositions de l'avant-projet de loi et sans lien avec les exigences de l'article 23.2 du RGPD.

Dérogation à l'article 20 de la LTD

82. L'article 38 prévoit une dérogation à l'obligation à de formaliser par voie de protocole les transferts de données à caractère personnel tant dans le chef des autorités qui communiqueront des données à l'autorité de certification de cybersécurité et aux autorités visées à l'article 5, §2 de l'avant-projet de loi que dans le chef de ces dernières.

83. L'Autorité rappelle que l'obligation de formaliser un échange de données visée à l'article 20 de la LTD ne s'applique pas à un échange ponctuel de données[20] ; ce qui serait le cas en cas d'application de l'article 29 du CiCr (autorités judiciaires).

[19] Ibidem

[20] Recommandation 02/2020 du 31 janvier 2020 de l'Autorité relative à la portée de l'obligation de conclure un protocole afin de formaliser les communications de données à caractère personnel en provenance du secteur public fédéral, p.16.

84. Pour pourvoir déroger à cet article 20 de la LTD, la norme doit encadrer le flux structurel de données à caractère personnel visé et ce, de façon prévisible et conforme aux principes de nécessité et de proportionnalité ; ce qui nécessite de « *prévoir explicitement qui (destinataire(s)) se voit transmettre quoi (catégories des données communiquées), quand et pourquoi (finalités et modalités de la communication)* »[21] dans le respect des principes de nécessité et de proportionnalité ; ce qui doit être fait au niveau des dispositions de l'avant-projet de loi qui encadrent ces communications de données par l'Autorité nationale de certification de cybersécurité. Il est à ce sujet renvoyé aux observations précitées de l'Autorité relatives aux articles 16 et 17 de l'avant-projet de loi qui encadrent lesdites communications structurelles de données.

85. Quant aux collectes structurelles de données à caractère personnel que l'Autorité nationale de certification de cybersécurité et les autorités visées à l'article 5, §2 réaliseraient auprès des autorités sectorielles (cf. supra) pour l'exercice des missions de service public prévues par le Règlement cybersécurité, elles doivent répondre aux mêmes critères de prévisibilité pour que ces autorités sectorielles soient dispensées de les formaliser par un protocole au sens de l'article 20 de la LTD. A défaut d'être prévues par les normes qui encadrent ces autorités sectorielles (ce qu'il appartient à l'auteur de l'avant-projet de loi de vérifier), les modalités précitées desdites communications doivent être prévues par le présent avant-projet de loi pour autant qu'elles portent sur des données à caractère personnel.

Par ces motifs,

L'Autorité

Considère que l'avant-projet de loi soumis pour avis doit être adaptée en ce sens :

1. Révision des articles 6 §1 et 3, 7, 16 §2 et 3, 17 §1 et 3, 36, §1 et 3, 4° et 38 qui prévoient les échanges de données afin de les circonscrire adéquatement au strict nécessaire et proportionné au regard des objectifs du Règlement cybersécurité ou de missions de services publics connexes touchant directement à la cybersécurité conformément aux considérations générales de l'avis et aux considérations particulières relatives à ces dispositions en projet (cons. 6 à 14 et 19, 20, 37, 40, 43 , 55, 85) ;

2. Imposition d'une obligation d'information spécifique à l'Autorité nationale de certification conformément au considérant 15 ;

[21] Ibidem, p.15

3. Suppression de la mission de délivrance des certificats du champ d'application de la dérogation au devoir de confidentialité et au secret professionnel (cons. 23) ;

4. Encadrement des dérogations au devoir de confidentialité, nécessaires à la réalisation des missions d'inspection l'autorité nationale de certification et des autorités visées à l'article 5, §2, conformément au considérant 26 ;

5. Mise en place de garanties adéquates pour les éventuelles collectes de données, nécessaires à l'exercice de ces missions d'inspection, couvertes par le secret professionnel conformément au considérant 27 ;

6. Précision de l'article 13, §2 relatif à la collecte d'informations du service d'inspection conformément au considérant 31 ;

7. Ajout de garanties pour la préservation des droits et libertés des clients (personnes physiques) des prestataires ICT contrôlés (ou les personnes physiques clientes de ces clients) au regard des collectes et communications légitimes du service d'inspection (cons. 33, 38, 67) ;

8. Imposition du respect du principe de proportionnalité dans l'exercice des missions d'inspection (cons. 34) ;

9. Motivation du caractère nécessaire de la dérogation au principe de confidentialité des communications électroniques et limitation aux hypothèses strictement nécessaires, encadrement de cette dérogation conformément aux considérants 49 et 50 (cons. 45 à 50)

10. Suppression de la description des catégories de traitements de données à caractère personnel (cons. 53 et 54) ;

11. Rectification de la description des finalités des traitements de données de l'autorité nationale de certification de cybersécurité et des autorités visées à l'article 5, §2 en projet conformément au considérant 55;

12. Précision de la qualification du responsable du traitement conformément aux considérants 56 et 57.

13. Suppression des articles 36, §2 en projet (cons. 58 à 64) ;

14. Précision exhaustive des catégories de données que l'Autorité nationale de certification de cybersécurité et les autorités désignées conformément à l'article 5, §2 traiteront dans l'exercice des missions que l'avant-projet de loi leur confie conformément aux considérants 61 et s. ;

15. Adaptation des catégories de personnes concernées à propos desquelles les autorités visées à l'article 5 traiteront des données conformément aux considérants 66 et 67 ;

16. Précision de l'article 39 en projet relatif à la durée de conservation des données conformément au considérant 69 ;

17. Limitation des droits des personnes concernées consacrés par le RGPD auxquels il est dérogé aux seuls droits dont l'exercice met en péril les missions d'inspection et encadrement adéquat de ces dérogations à ces droits et à l'obligation de protocole d'échange de données prévu à l'article 20 de la LTD conformément aux considérants 73 à 81.

Pour le Centre de Connaissances,
(sé) Rita Van Nuffelen – responsable a.i. du Centre de Connaissances