Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 51/2022 du 9 mars 2022

Objet : Avis relatif à un avant-projet de loi *modifiant le Code belge de la Navigation concernant la sûreté maritime* (articles 8 et 21) (CO-A-2022-019)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après "l'Autorité"), en présence de Madame Marie-Hélène Descamps et de Messieurs Yves-Alexandre de Montjoye et Bart Preneel ;

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 "la 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* (Règlement général sur la protection des données, ci-après le "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 "la LTD") ;

Vu la demande d'avis de Monsieur Vincent Van Quickenborne, , Vice-premier Ministre et Ministre de la Justice et de la Mer du Nord (ci-après : le demandeur), reçue le 14/01/2022 ;

Émet, le 9 mars 2022, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le 14/01/2022, le demandeur a sollicité l'avis de l'Autorité sur un avant-projet de loi *modifiant le Code belge de la Navigation concernant la sûreté maritime* (ci-après : le projet).

2. Le projet a pour objet de soumettre la sécurité maritime à une révision complète et approfondie.

Contexte

3. Dans le cadre de la sûreté maritime, il convient d'abord d'attirer l'attention sur la Convention internationale pour la sauvegarde de la vie humaine en mer (ci-après : la Convention SOLAS – *Safety of Life at Sea*) et le Code international pour la sûreté des navires et des installations portuaires (ci-après : le Code ISPS - *International Ship and Port Facility Security*). Le Code ISPS est composé de trois parties : le préambule, la partie A et la partie B. La partie A contient les règlements obligatoires pour tous les pays qui ont ratifié la Convention SOLAS alors que la partie B contient des recommandations et des lignes directrices pour la mise en œuvre de la partie A.

4. Le Règlement (CE) N° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 *relatif à l'amélioration de la sûreté des navires et des installations portuaires* (ci-après : le Règlement ISPS) oblige les États membres européens à mettre effectivement en œuvre le Code ISPS[1].

5. Le Code ISPS et le Règlement ISPS se limitent cependant aux mesures de sûreté à bord des navires et dans les installations portuaires. La Commission européenne a toutefois considéré que pour protéger de manière optimale les industries maritimes, les mesures nécessaires devaient également être prises dans les zones environnantes pour assurer la sécurité. L'initiative de la Commission européenne a abouti à la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 *relative à l'amélioration de la sûreté des ports* (ci-après : la Directive sur la sûreté portuaire).

6. Le Règlement ISPS et la Directive sur la sûreté portuaire ont été mis en œuvre en Belgique par la loi du 5 février 2007 *relative à la sûreté maritime* et l'arrêté royal du 21 avril 2007 *relatif à la sûreté maritime*. La loi du 5 février 2007 susmentionnée a été abrogée et reprise dans le Code belge de la Navigation.

[1] Voir l'article 3.5 du Règlement ISPS.

7. Toutefois, comme il ressort de l'Exposé des motifs, après 15 ans, il était temps de revoir et de compléter la réglementation existante, compte tenu des principaux problèmes révélés au terme d'une enquête auprès des acteurs de la sécurité maritime. À cette fin, les objectifs principaux suivants ont été identifiés :
   - réformer et moderniser la structure de la sûreté maritime en Belgique ;
   - améliorer la sûreté des ports et des installations portuaires au moyen de nouvelles mesures de sûreté (dont le traitement de données biométriques) pour lutter contre le crime organisé ;
   - contrôler le respect de l'interdiction de port conformément à l'article 4, § 3*bis* de la loi du 24 février 1921 *concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes* (ci-après : la Loi relative aux drogues) ;
   - créer un cadre légal en ce qui concerne l'utilisation de caméras de surveillance dans la partie belge de la Mer du Nord.

8. Lors de la rédaction du projet, les éléments suivants méritant une attention particulière afin de pouvoir créer un cadre légal ont également été avancés :
   - l'applicabilité de la loi du 21 mars 2007 *réglant l'installation et l'utilisation de caméras de surveillance* (ci-après : la Loi caméras) dans la partie belge de la Mer du Nord ;
   - la recommandation n° 01/2021 de l'Autorité *relative au traitement de données biométriques*[2].

II. EXAMEN QUANT AU FOND

a. <u>Remarque préliminaire concernant la base juridique</u>

9. En plus de devoir être nécessaire et proportionnée, toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) doit répondre aux exigences de prévisibilité et de précision afin que les personnes concernées au sujet desquelles des données sont traitées aient une idée claire du traitement de leurs données. En application de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la *Constitution* et 8 de la CEDH, une telle norme légale doit décrire les éléments essentiels des traitements allant de pair avec l'ingérence de l'autorité publique. Dans ce cadre, il s'agit au moins :
   - de la (des) finalité(s) précise(s) et concrète(s) des traitements de données ;
   - de la désignation du responsable du traitement.

[2] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/recommandation-01-2021-du-1-decembre-2021.pdf.

Si les traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique représentent une ingérence importante dans les droits et libertés des personnes concernées, la disposition légale doit également comprendre les éléments essentiels (complémentaires) suivants :

- les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
- les catégories de personnes concernées dont les données à caractère personnel seront traitées ;
- les catégories de destinataires des données à caractère personnel ainsi que les conditions dans lesquelles ils reçoivent les données et les motifs y afférents ;
- le délai de conservation maximal des données à caractère personnel enregistrées ;
- l'éventuelle limitation des obligations et/ou droits mentionné(e)s aux articles 5, 12 à 22 et 34 du RGPD.

10. Les traitements de données qui seront instaurés à la suite du projet représentent une ingérence importante dans les droits et libertés des personnes concernées. Les traitements concernent en effet des catégories particulières de données à caractère personnel au sens des articles 9 et 10 du RGPD, ils ont lieu à des fins de surveillance et de contrôle et peuvent entraîner des conséquences négatives pour les personnes concernées. Il est donc requis que tous les éléments essentiels du traitement énumérés ci-dessus soient repris dans le projet.

11. Les dispositions qui concernent le traitement de données à caractère personnel et celles nécessaires pour pouvoir comprendre le contexte du traitement des données font l'objet d'un commentaire article par article repris ci-après. Sauf indication contraire, les articles concernent toujours les articles du projet et pas ceux actuellement en vigueur dans le Code belge de la Navigation.

b. <u>Article 8 du projet</u>

12. L'article 8 du projet remplace le chapitre 2 du titre 5 du livre 2 du Code belge de la Navigation et prévoit la mise en œuvre du Règlement ISPS et la transposition de la Directive sur la sûreté portuaire.

13. Le projet de chapitre 2 du titre 5 du livre 2 du Code belge de la Navigation a pour objectif (1°) *l'introduction de mesures visant à améliorer la sûreté des navires de mer utilisés dans le commerce international et le trafic intérieur et des installations portuaires associées contre le danger d'actions illicites ;* (2°) *le renforcement de la sûreté face aux menaces d'incidents de sûreté par l'établissement de règles relatives à la sûreté ;* (3°) *la protection des personnes travaillant dans*

un port ou une installation portuaire, sur un ouvrage de construction ou de génie civil dans les zones maritimes ou à bord des navires de mer ; (4°) *l'établissement des mesures visant à garantir la sûreté des navires de mer et des ouvrages de construction et de génie civil, y compris les câbles et les pipelines, dans les zones maritimes belges ;* (5°) *l'établissement de mécanismes pour le respect du présent chapitre*.

Article 2.5.2.3 Notions

14. Dans le contexte du projet, la notion d' 'action illicite' est cruciale. En effet, comme cela ressort des objectifs généraux (voir le point 13), les nouvelles mesures de sûreté, qui impliquent dans une large mesure un traitement de données à caractère personnel, ciblent la protection des navires de mer et des installations portuaires contre le danger d'actions illicites.

15. Le risque de certaines actions illicites doit également être pris en considération lors de l'évaluation de la proportionnalité des mesures de sûreté adoptées. En effet, vu la grande variété des installations portuaires, chacune doit être protégée d'une manière qui lui soit propre[3].

16. Le point 15° de l'article susmentionné définit une 'action illicite' comme suit : "*toute action qui, compte tenu de sa nature ou de son contexte, pourrait causer des dommages aux navires de mer du trafic maritime international et national, aux passagers ou à la cargaison, ou aux ports ou installations portuaires concernés, y compris l'utilisation de navires de mer pour faire entrer ou sortir de Belgique des articles ou produits interdits via les ports et installations portuaires ou pour permettre à des personnes ou des animaux d'embarquer ou de débarquer sans autorisation, ou toute activité connexe.*"

17. L'Exposé des motifs considère concrètement les activités suivantes comme illicites : le terrorisme, la piraterie, l'espionnage, le sabotage, le trafic de drogue, le commerce de produits de contrefaçon, la contrebande de personnes, le commerce illégal d'animaux exotiques. Bien que l'Autorité estime que la lutte contre de telles activités constitue une finalité licite, elle considère néanmoins que la formulation actuelle de l'article laisse une marge d'appréciation trop large. Vu la nature des traitements de données qui peuvent, le cas échéant, être mis en œuvre dans le cadre de la sûreté des navires et des installations portuaires, il est recommandé d'au moins spécifier explicitement dans la loi les catégories d'actions illicites. Le passage "*toute action qui … pourrait causer des dommages aux ...*" donne à tort l'impression que lors de la réalisation d'une évaluation de la sûreté

[3] L'Exposé des motifs donne l'exemple suivant : "*Un terminal à conteneurs ou un terminal fruitier dont les importations proviennent d'Amérique latine doit être beaucoup plus protégé qu'un terminal de sable qui ne livre que du sable dragué de la mer du Nord. Toutefois, certaines exigences minimales devront s'appliquer à tous, comme les barrières physiques et la vérification de leur intégrité, ainsi que le contrôle obligatoire de l'accès de tous les véhicules et de toutes les personnes cherchant à entrer dans une installation portuaire.*"

et de l'élaboration d'un plan de sûreté, les acteurs visés peuvent déterminer, à leur guise, quelles actions relèvent du champ d'application de la loi. Cela peut donner lieu à des abus et cela est contraire au projet d'harmoniser autant que possible la sûreté des ports et installations portuaires belges, des navires et de la Mer du Nord.

18. Pour le reste, l'Autorité considère que les notions définies n'appellent pas de remarque particulière en ce qui concerne le traitement de données à caractère personnel.

Article 2.5.2.4 Champ d'application

19. L'article précité précise tout d'abord, conformément aux dispositions du Règlement ISPS, les séries de navires de mer qui ne relèvent pas du champ d'application du projet.

20. Ensuite, le paragraphe 2 définit l'application territoriale à l'intérieur du territoire belge. À cette fin, il est spécifié que tout endroit où les navires de mer interagissent avec la terre est considéré comme une 'installation portuaire'.

21. Les autres paragraphes concernent respectivement les ouvrages de construction et de génie civil ainsi que les câbles ou les pipelines dans les zones maritimes belges, les exceptions militaires et l'interdiction de recevoir des navires de mer s'il n'existe pas de plan de sécurité valide dans le port ou l'installation portuaire.

22. L'Autorité en prend acte.

Articles 2.5.2.5 – 2.5.2.14 (Section 2 - Autorités)

23. Les articles précités traitent de la composition, du fonctionnement et de l'ensemble de tâches respectivement de l'Autorité Nationale de Sûreté Maritime (ci-après : ANSM) et des Comités locaux de la Sûreté maritime[4] (ci-après : CLSM).

Articles 2.5.2.15 – 2.5.2.46 (Section 3 – Sûreté portuaire et Section 4 - Sûreté des installations portuaires)

24. Les sections 3 et 4 contiennent la réglementation concernant la réalisation d'une évaluation de la sûreté et l'élaboration d'un plan de sûreté pour les ports et les installations portuaires.

[4] Ayant pour président l'agent de sûreté portuaire visé à l'article 9 de la Directive sur la sûreté portuaire (PSO - *Port Security Officer*).

25. L'évaluation de la sûreté constitue la base des travaux ultérieurs sur le plan de sûreté et sa mise en œuvre. En ce qui concerne l'évaluation de la sûreté portuaire, il faut notamment tenir compte des particularités des différentes parties du port (des installations portuaires) ainsi que des zones adjacentes si ces dernières ont une incidence sur la sûreté du port. À cette fin, il faut au moins définir les éléments suivants[5] :

"1° la détermination et l'évaluation de l'infrastructure et des moyens de production importants qu'il convient de protéger ;

2° l'identification des ***risques d'actions illicites*** *;*

3° l'identification des menaces possibles pour l'infrastructure et les moyens de production et la probabilité d'occurrence, en vue de déterminer et de hiérarchiser les mesures de sûreté ;

4° la détermination, la sélection et la hiérarchisation des mesures et des changements de procédure en vue de réduire les vulnérabilités en matière de sûreté et leur niveau d'efficacité ;

5° l'identification des faiblesses, y compris les facteurs humains, dans l'infrastructure, les politiques et les procédures ;

6° l'analyse des risques des éléments susceptibles d'être victimes d'espionnage, de terrorisme et de sabotage à la suite d'influences étrangères au moyen d'une collaboration publique ou privée."

26. Après approbation de l'évaluation de la sûreté par l'ANSM[6], un plan de sûreté qui décrit concrètement les mesures de sûreté (dont les traitements visés de données à caractère personnel)[7] (qui doit également être soumis à l'approbation de l'ANSM) est élaboré. Il en résulte que l'ANSM endosse la responsabilité finale de vérifier la proportionnalité des mesures proposées[8]. Dans ce cadre, l'Autorité souligne une fois de plus la nécessité de concrétiser davantage la notion (de risques) d'actions illicites dans le projet (point 17). Les constatations à cet égard jouent en effet un rôle important lors de l'établissement de mesures de sûreté appropriées.

27. Enfin, dans ce cadre, l'Autorité souhaite encore attirer l'attention sur l'obligation, dans le chef de l'agent de sûreté d'une installation portuaire (ci-après : PFSO - *Port Facility Security Officer*) - qui se charge de réaliser une évaluation de la sûreté de l'installation portuaire et d'élaborer un plan de sûreté -, de satisfaire aux exigences de formation conformément à l'article 2.5.2.39. À cet effet, le PFSO doit passer un examen auprès d'un organisme de sûreté reconnu ou d'un organisme de formation reconnu[9] conformément aux modalités déterminées par le Roi. L'organisation et le

[5] Article 2.5.2.15, voir en outre les explications de cet article dans l'Exposé des motifs où sont abordés en détail les différents aspects de sûreté qui doivent être pris en considération.

[6] Voir les articles 2.5.2.16, 2.5.2.31 et 2.5.2.35.

[7] Concernant les aspects de sûreté du plan de sûreté, voir les explications de l'article 2.5.2.34 dans l'Exposé des motifs.

[8] Dans ce cadre, on peut également faire référence aux articles 2.5.2.6, § 2, 2° ("*L'ANSM est compétent* [NdT : il convient de lire "compétente"] *pour les questions de sûreté dans les ports et les installations portuaires*") ; 2.5.2.6, § 3 et 2.5.2.22.

[9] Voir la section 8 - Organismes de sûreté et organismes de formation reconnus (les articles 2.5.2.69 - 2.5.2.76).

déroulement de tels examens impliquent un traitement de données à caractère personnel des candidats. Bien que ce traitement n'implique pas nécessairement une ingérence importance dans les droits et libertés des personnes concernées, l'Autorité souligne la nécessité d'en définir les éléments essentiels dans l'arrêté royal qui vise à exécuter l'article susmentionné[10].

28. La même remarque s'applique en ce qui concerne les instructions de l'ANSM telles que visées aux articles 2.5.2.44 et 2.5.2.66 dans la mesure où celles-ci ont été ratifiées par le Roi conformément respectivement aux articles 2.5.2.45 et 2.5.2.67 et la formation de l'agent de sûreté de l'armateur (ci-après : CSO - *Company Security Officer*) et du navire (ci-après : SSO - *Ship Security Officer*) conformément aux articles 2.5.2.61 et 2.5.2.62.

Articles 2.5.2.77 – 2.5.2.81 (Section 9 – Plate-forme ISPS)

29. Les articles susmentionnés régissent l'échange électronique d'informations entre tous les acteurs concernés par la sûreté maritime pour la mise en œuvre du projet de chapitre 2 du Code belge de la Navigation et de ses arrêtés d'exécution ainsi que le stockage des informations.

30. Actuellement, une combinaison de différentes méthodes de communication est utilisée pour traiter l'échange d'informations entre les différents acteurs en ce qui concerne les avis motivés, les approbations, les signalements d'incidents, … Il est précisé dans l'Exposé des motifs que cet amalgame de méthodes de communication ne satisfait pas aux exigences imposées par le Règlement ISPS et la Directive sur la sûreté portuaire de traiter les informations en matière de sûreté d'une façon sécurisée et uniforme.

31. L'ANSM assure la gestion de la plate-forme ISPS et doit contribuer activement à l'efficacité du fonctionnement sûr de la plate-forme. Par souci d'exhaustivité, l'Exposé des motifs précise que la plate-forme sera développée dans le respect des dispositions 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* (la loi RSI). L'Autorité en prend acte.

32. L'article 2.5.2.78 définit les objectifs de la plate-forme ISPS :

> *"1° le stockage, le suivi et l'approbation de toutes les évaluations de la sûreté mentionnées dans le présent chapitre ;*
> *2° le stockage, le suivi et l'approbation de tous les plans de sûreté mentionnés dans le présent chapitre ;*

[10] Concernant l'organisation d'épreuves d'aptitude ou d'examens prescrit(e)s par la loi, l'Autorité renvoie à son avis n° 86/2021. Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/avis-n-86-2021.pdf.

*3° le signalement, l'enregistrement et le suivi des **incidents de sûreté***[11] *;*

*4° le signalement, l'enregistrement et le suivi des **exercices** ;*

5° l'échange d'informations entre les acteurs concernés ;

6° la saisie, l'enregistrement et le suivi des rapports d'inspection par les différents services ;

(…)

12° l'automatisation et la fourniture des informations de sûreté par les navires étrangers ;

*13° **le stockage des données du contrôle d'accès** ;*

*14° **la vérification du respect de l'interdiction visée à l'article 4, § 3bis, de la loi du 24 février 1921** concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes et à l'article 4.1.2.48 du Code belge de la Navigation ;*

*15° **la vérification du respect de l'interdiction imposée aux personnes qui, en vertu du chapitre X de la loi du 20 juillet 1990** relative à la détention préventive, ont reçu la condition de ne pas se rendre dans un port ou une installation portuaire ;*

*16° la mise à jour des **habilitations de sûreté** et des demandes requises par le présent chapitre ;*

*17° **la mise à jour de la liste des membres de l'ANSM, du CLSM, de la Cellule de la sûreté maritime, du PFSO et du CSO.**"*

33. Bien que cette énumération d'objectifs permette dans un certain sens d'avoir une idée des données qui doivent être reprises dans la plate-forme ISPS, on ne sait pas du tout clairement quels acteurs assurent concrètement la réalisation de quelles finalités, ni à quelles données ces acteurs ont le

[11] Dans le cadre d'une demande d'informations complémentaires, le demandeur a fourni les explications suivantes concernant la notion d' 'incidents de sûreté' : "*Une définition de l'incident de sûreté figure dans la Prescription 1, point 1, au point 13° du Chapitre XI-2 de la Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS). Celle-ci a été reprise à l'Annexe 1 du Règlement 725/2004 (Règlement ISPS). La définition qui y figure est la suivante :*

"13. Incident de sûreté désigne tout acte suspect ou toute circonstance suspecte qui menace la sûreté d'un navire, y compris une unité mobile de forage au large et un engin à grande vitesse, ou d'une installation portuaire ou d'une interface navire/port ou d'une activité de navire à navire".

Dans le présent projet de loi [NdT : dans la version néerlandaise] *concernant la sûreté maritime, on a toutefois explicitement choisi de remplacer là où c'était possible le terme 'veiligheid' par le terme 'beveiliging', et ce afin d'indiquer que les règlements spécifiques régis dans le présent projet ne peuvent pas être invoqués pour augmenter la sécurité (par ex. afin de prévenir les accidents du travail) mais que la finalité doit toujours être associée à la sûreté du navire, de l'installation portuaire ou des personnes présentes. (...)*

L'article 15.11 de la partie B du Code ISPS précise que toutes les menaces possibles doivent être prises en considération et donne une liste non limitative d'incidents de sûreté.

(…)

*Ces mentions contiennent donc toutes les informations nécessaires pour évaluer l'incident de sûreté. **Cela concerne les faits mais ne comporte aucune donnée à caractère personnel de suspects**. Les données à caractère personnel seront toutefois reprises dans les procès-verbaux établis par les services compétents lors de l'incident de sûreté si la personne est suspectée d'avoir commis un délit. En effet, tous les incidents de sûreté ne génèrent pas non plus un délit. Ainsi, un grillage qui a été endommagé par un accident ou une rafale de vent constituera un incident de sûreté mais pas un délit. Les données du déclarant (dans presque tous les cas, il s'agira du PFSO, de son adjoint(e) ou de l'agent de surveillance de l'organisme de sûreté reconnu) seront toutefois bien entendu communiquées de manière à pouvoir prendre contact pour l'évaluation ultérieure qui est requise."* [Traduction libre réalisée par le service de traduction du Secrétariat Général de l'Autorité en l'absence de traduction officielle]

cas échéant accès. Il semble en effet difficilement justifiable que chaque PSO, PFSO ou CSO ait accès sans condition aux données du contrôle d'accès de toutes les installations portuaires, de tous les incidents de sûreté ou exercices, à toutes les données relatives au contrôle de l'interdiction de port, aux habilitations de sécurité de certaines personnes, ...

34. Cela s'applique d'autant plus qu'on ne sait pas tout à fait clairement quel est le lien entre l'article 2.5.2.89 - concernant l'accès aux données à caractère personnel visées à l'article 2.5.2.**88**[12] pour les finalités visées à l'article 2.5.2.**86**[13] - et l'accès à la plate-forme ISPS. En effet, comme cela semble raisonnablement découler des objectifs de la plate-forme ISPS, contrairement à ce qui ressort de l'article 2.5.2.89, d'autres acteurs que l'ANSM, les CLSM, la Cellule de la sûreté maritime, le ministère public, les services de renseignement et les services d'inspection visés à l'article 4.2.4.4 auront accès aux données (à caractère personnel) de la plate-forme ISPS.

35. Dès lors, l'Autorité demande de **spécifier dans le projet quels acteurs peuvent consulter la plate-forme ISPS pour quelles finalités**. En ce qui concerne les données relatives aux évaluations de la sûreté et aux plans de sûreté, aux incidents de sûreté, aux exercices, aux contrôles d'accès, à l'interdiction de port et aux personnes visées au point 17° de l'article 2.5.2.78, il est possible par exemple de travailler à l'aide d'environnements partitionnés par installation portuaire, permettant ainsi d'organiser l'accès aux données de façon graduelle : l'ANSM - en tant que responsable de la gestion de la plate-forme - a connaissance de toutes les données ; les CLSM ont accès aux données relatives aux ports qui relèvent de leur compétence ; le PFSO a accès aux données relatives à son installation portuaire, ...

36. Selon l'article 2.5.2.81, afin d'avoir accès à une installation portuaire, il faut vérifier à l'entrée si la personne qui souhaite y accéder figure sur la plate-forme ISPS en tant que personne à laquelle une interdiction a été imposée conformément à l'article 4, § 3*bis* de la Loi relative aux drogues ou à l'article 4.1.2.48 du Code belge de la Navigation, ou à laquelle en vertu du chapitre X de la loi du 20 juillet 1990 *relative à la détention préventive*, la condition de ne pas se rendre dans un port ou une installation portuaire a été imposée.

37. Une telle interdiction portuaire est une sanction autonome par laquelle il est temporairement interdit de se rendre dans un ou plusieurs ports et cela suppose logiquement un contrôle effectif de son respect. L'Autorité prend acte du fait que les données à caractère personnel qui seront traitées dans le cadre de ce contrôle (voir à cet égard également le commentaire des articles 2.5.2.86 à 2.5.2.95) seront centralisées dans la plate-forme ISPS. Il est en effet préférable

[12] Au moment de rédiger le présent avis, l'article 2.5.2.89 renvoie à tort à l'article 2.5.2.84.

[13] Au moment de rédiger le présent avis, l'article 2.5.2.89 renvoie à tort à l'article 2.5.2.82.

que les autorités (judiciaires) qui ont imposé une telle sanction ne doivent transmettre ces informations qu'une seule fois à la plate-forme centralisée ; plutôt que de devoir contacter séparément chaque installation portuaire ou port visé(e). Cela favorise la sécurité de l'information. L'Autorité souligne toutefois, compte tenu du fait qu'une interdiction de port peut être imposée pour un ou plusieurs ports ou une ou plusieurs installations portuaires, que ces données ne peuvent être accessibles que pour les acteurs qui assurent le contrôle d'accès du (des) port(s) ou installations portuaires visé(e)(s)[14] (voir également le point 35). En outre, l'Autorité estime que la plate-forme ISPS a pour but d'**enregistrer** les données utiles relatives à l'interdiction de port en vue du contrôle du respect de celle-ci. Le contrôle en soi, tel que cela semble résulter actuellement des dispositions susmentionnées, n'est toutefois pas une finalité de la plate-forme ISPS. L'Autorité demande d'adapter adéquatement les points 14° et 15° en ce sens.

38. En conclusion, l'Autorité estime que, compte tenu de la fonction centrale de la plate-forme dans le contexte global de la sûreté, la réglementation concernant la plate-forme ISPS peut et doit être mieux alignée sur les dispositions relatives au traitement de données à caractère personnel (dans lesquelles, à quelques exceptions près, la plate-forme n'est mentionnée nulle part). Sans porter préjudice aux avantages d'une plate-forme centralisée pour l'échange de données, on ne sait toujours pas clairement actuellement quelles finalités parmi celles avancées peuvent donner lieu à un traitement de (quelles) données à caractère personnel et par quels acteurs. Cela n'est pas compatible avec l'article 6.3 du RGPD, lu à la lumière du considérant 41 et de l'article 22 de la *Constitution*.

Article 2.5.2.82 - 2.5.2.83 (Images de caméra)

39. L'article 2.5.2.82 dispose que "*Les caméras de surveillance installées par les exploitants des ports ou des installations portuaires doivent être conformes aux dispositions de la* Loi caméras".

40. L'article 3 de la Loi caméras établit que l'installation et l'utilisation de caméras de surveillance (privées) ne peuvent avoir pour finalité que :

- *"1° prévenir, constater ou déceler des infractions contre les personnes ou les biens, ou*
- *2° prévenir, constater ou déceler des incivilités au sens de l'article 135 de la nouvelle loi communale, contrôler le respect des règlements communaux ou maintenir l'ordre public."*

[14] En ce sens, l'Exposé des motifs dispose ce qui suit : "*Du fait que l'interdiction portuaire peut être imposée pour un ou plusieurs ports ou installations portuaires, ces données doivent être contrôlées et encodées de façon très correcte du côté du gouvernement. Une personne qui a reçu une interdiction pour le port A doit en effet pouvoir obtenir l'accès dans le port B sans qu'il ne puisse y avoir la moindre indication que cette personne a été condamnée à une interdiction portuaire.*"

L'article 9 de cette même loi définit les modalités du traitement des images de telles caméras de surveillance.

41. Étant donné que le projet ne spécifie aucune particularité concernant l'installation de caméras de surveillance, les dispositions de la Loi caméras s'appliquent intégralement. L'Autorité en prend acte.

42. L'article 2.5.2.83, § 1er dispose que "*L'utilisation de* ***caméras intelligentes*** *en vue de la reconnaissance automatique des plaques d'immatriculation par les exploitants des ports et des installations portuaires est autorisée.*" En outre, par dérogation à l'article 8/1 de la Loi caméras, l'utilisation de telles caméras de surveillance intelligentes est également autorisée en vue de la **reconnaissance automatique des navires**.

43. Dans le cadre d'une demande d'informations complémentaires, le demandeur spécifie que les caméras intelligentes (aussi désignées en tant que caméras ANPR) qui peuvent être installées par les exploitants du port servent uniquement à enregistrer des plaques d'immatriculation, conformément aux règles qui leur sont applicables. L'article 8/1 de la Loi caméras précise en ce sens : "*L'utilisation de caméras de surveillance intelligentes couplées à des registres ou à des fichiers de données à caractère personnel n'est autorisée qu'en vue de la reconnaissance automatique des plaques d'immatriculation,* ***à condition que le responsable du traitement traite ces registres ou ces fichiers dans le respect de la réglementation relative à la protection de la vie privée****.*" Cela n'affecte en rien les autres obligations qui reposent sur le responsable du traitement conformément à la Loi caméras. En la matière, l'Autorité souligne toutefois que toute autorisation d'utiliser des caméras intelligentes pour cette finalité semble peu judicieuse dans la mesure où les acteurs concernés n'ont pas accès aux données des plaques d'immatriculation dans le répertoire des véhicules qui est conservé par la Direction générale Transport routier et Sécurité routière du SPF Mobilité et Transports[15]. Il incombe donc au responsable du traitement de vérifier s'ils peuvent avoir accès à ces données conformément à la réglementation pertinente[16].

44. De plus, l'Autorité rappelle l'obligation pour le responsable du traitement de réaliser une analyse d'impact relative à la protection des données, conformément à l'article 35 du RGPD, lorsqu'il prévoit un traitement de données à caractère personnel qui, vu sa nature, sa portée, son contexte et ses finalités, implique un risque élevé pour les droits et libertés des personnes physiques.

---

[15] Voir la remarque au point 26 de l'avis n° 53/2017 de la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité (consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/avis-n-53-2017.pdf) et les articles 6 et 7 de l'arrêté royal du 20 juillet 2001 *relatif à l'immatriculation de véhicules*.

[16] En la matière, l'Autorité renvoie à la loi du 19 mai 2010 *portant création de la Banque-Carrefour des véhicules* et à l'arrêté royal du 20 juillet 2001 *relatif à l'immatriculation de véhicules*.

L'installation et l'utilisation de caméras ANPR constituent en effet une collecte de données à grande échelle au moyen de nouvelles technologies afin d'analyser la localisation ou les déplacements de personnes physiques[17]. Concernant les modalités d'exécution d'une analyse d'impact relative à la protection des données, l'Autorité renvoie à la recommandation n° 01/2018[18] de son prédécesseur en droit, la Commission de la protection de la vie privée, et au Guide AIPD de l'Autorité[19]. Par analogie avec l'analyse d'impact relative à la protection des données qui doit être réalisée dans le cadre du traitement de données biométriques, il convient de recommander que l'analyse d'impact relative à la protection des données pour l'installation de caméras de surveillance (intelligentes) soit également reprise dans l'évaluation de la sûreté du port (des installations portuaires) (voir le point 53).

45. Quant à la reconnaissance automatique des navires, le demandeur précise ensuite qu'il existe dans les ports une obligation pour tous les navires qui y naviguent (à l'exception des navires de plaisance) de disposer de ce qu'on appelle un AIS-transponder (`*automatic identification system*'). Ce système est relié au navire et donne une identification de son numéro d'immatriculation et de son numéro MMSI (*Maritime Mobile Service Identification*) (l'autorisation de station qui a été attribuée par l'IBPT en Belgique[20]). La reconnaissance automatique pour la navigation implique donc que si un navire est détecté dans le port, les données relatives au propriétaire ou à l'exploitant de ce navire peuvent être réclamées, via la connexion AIS, auprès des services belges compétents s'il s'agit d'un navire belge, auprès des services étrangers pour les navires étrangers, ou auprès d'organisations agréées à cet effet (par exemple Lloyds) qui conservent les données de tous les navires de mer. Bien que cette connexion AIS se fasse à l'aide de signaux radio, il ressort de l'Exposé des motifs qu'il importe que les signaux AIS soient reliés à des images de caméra de manière à pouvoir détecter également les navires sans AIS-transponder.

46. Étant donné que la connexion AIS et les images de caméra sont toutefois des systèmes distincts, l'Autorité estime que la nécessité d'utiliser des caméras intelligentes au sens de l'article 2, 4°/3 de la Loi caméras - à savoir une "*caméra de surveillance qui comprend également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies*" - pour la reconnaissance automatique des navires n'est pas suffisamment démontrée. En effet, si un navire, en dépit de la réglementation

[17] Conformément au point 6.4) de la décision n° 01/2019 du Secrétariat Général de l'Autorité, la réalisation d'une analyse d'impact relative à la protection des données est obligatoire pour de tels traitements. Cette décision, qui exécute l'article 35.4 du RGPD, peut être consultée via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf.

[18] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf.

[19] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf.

[20] Voir par exemple : https://www.vesselfinder.com/fr.

qui lui est applicable, ne dispose pas d'un AIS-transponder, le fait que ce navire soit filmé au moyen de caméras de surveillance 'ordinaires' peut suffire.

47. L'article 2.5.2.83, § 2 dispose que "*L'utilisation de caméras intelligentes conformément au paragraphe 1er est autorisée pour la vérification du respect du Règlement ISPS, du Code ISPS et du présent chapitre et ses arrêtés d'exécution, ainsi que pour la prévention des actions illicites et la garantie de la sûreté maritime.*"

48. Compte tenu de la portée des réglementations susmentionnées et de la nature des traitements à l'aide de caméras intelligentes (voir le point 44), l'Autorité estime que ce paragraphe laisse une (trop) large marge d'interprétation subjective. Dans la mesure où l'utilisation de caméras intelligentes est nécessaire pour contrôler le respect de certaines obligations, cela doit transparaître explicitement dans la loi.

Article 2.5.2.84 (Utilisation de données biométriques)

49. L'Exposé des motifs mentionne que plusieurs entreprises portuaires traitent déjà actuellement des données biométriques pour vérifier si une personne peut accéder à une installation portuaire déterminée ou à un réseau électronique déterminé. La recommandation n° 01/2021 de l'Autorité *relative au traitement de données biométriques* souligne que depuis l'entrée en vigueur du RGPD, la base juridique nécessaire à cet effet fait défaut dans la réglementation belge. Dans ce cadre, les auteurs du projet prétendent toutefois à tort que l'Autorité a accordé un délai d'1 an à ces entreprises pour soit mettre fin progressivement à l'utilisation des données biométriques, soit inciter le législateur à prévoir un cadre juridique. Non seulement un tel délai est incompatible avec le fonctionnement direct du RGPD au sein de l'ordre juridique belge mais il y a également lieu de constater qu'entre-temps, le RGPD est d'application depuis déjà 4 ans. Tout traitement de données biométriques qui a lieu sans base juridique valable engendre une violation du RGPD. Le passage en question doit purement et simplement être supprimé de l'Exposé des motifs.

50. Comme cela est expliqué de manière circonstanciée dans la recommandation n° 01/2021[21], dans la mesure où il entend autoriser l'utilisation de données biométriques pour certaines finalités en vertu de l'article 9.2.g) du RGPD, le législateur belge doit régir les modalités de ce traitement explicitement par une loi.

51. L'article 2.5.2.84 distingue trois finalités pour le traitement de données biométriques dans les ports ou les installations portuaires :

[21] Voir la sous-section 1.3.2 *Intérêt public important* de la recommandation n° 01/2021, p. 25 - 28.

- premièrement, les plans de sûreté peuvent - **sur la base d'éléments concrets dans les évaluations de la sûreté qui en démontrent la nécessité**[22] - prévoir que l'accès à une installation portuaire soit subordonné à la vérification des données biométriques pour toutes ou certaines catégories de visiteurs[23]. L'Exposé des motifs précise que l'utilisation de données biométriques est absolument nécessaire pour un contrôle d'accès correct. En effet, selon de 'récentes informations', un badge d'accès à une installation portuaire se paie jusqu'à 7 500 euros sur le marché noir. Cependant, dès lors que ce badge est lié à des données biométriques, la transmission de ce badge ne sera tout simplement plus possible ;
- deuxièmement, on peut prévoir que l'accès numérique à certains modules des réseaux et systèmes d'information du port (des installations portuaires) doive également se faire au moyen de données biométriques[24] ;
- troisièmement, les données biométriques peuvent être utilisées dans le cadre de la manutention de la cargaison (et plus précisément pour l'accès à un *straddle carrier* (chariot cavalier) ou élévateur de conteneurs qui est utilisé pour charger des navires et, le cas échéant, pour isoler des cargaisons suspectes d'une inspection[25]).

52. L'Autorité souligne que l'énumération des finalités entrant en ligne de compte n'est pas un sauf-conduit pour le traitement de données biométriques et qu'elle ne dispense nullement le responsable du traitement de son obligation d'étayer la nécessité et la proportionnalité du traitement de données. Comme cela a déjà été expliqué, une évaluation de la sûreté doit être mise en œuvre, dans laquelle notamment les risques d'actions illicites sont identifiés. Des éléments concrets (type de cargaison, origine du navire, infrastructure de l'installation, ...) devront être pris en considération lors de l'évaluation de la nécessité du traitement de données biométriques. En la

---

[22] Bien que cela pourrait être déduit des dispositions relatives aux évaluations de la sûreté et aux plans de sûreté et de l'Exposé des motifs, il semble recommandé de reprendre explicitement une précision en ce sens dans l'article précité.

[23] Pour l'application de cette réglementation, l'article 2.5.2.84, § 3 dispose qu'on entend par 'visiteur' "*quiconque, y compris les administrateurs et les membres du personnel, souhaite avoir accès à l'installation portuaire ou à des parties de l'installation portuaire à l'exception des passagers des navires de mer qui embarquent ou débarquent dans une installation portuaire pour le transport de passagers, et des membres de l'équipage des navires de mer.*"

[24] Extrait de l'Exposé des motifs : "*Par exemple, un membre du personnel qui a accès aux bonnes données peut s'assurer que les conteneurs sont placés à un certain endroit. En divulguant les codes PIN avec lesquels une cargaison particulière peut être prise en charge par le transporteur externe, cette cargaison peut à nouveau être sortie de l'installation portuaire assez facilement. Par conséquent, pour lutter efficacement contre la criminalité organisée, il est nécessaire de pouvoir identifier qui a eu accès à certaines informations et les a utilisées à des fins illicites.*

En l'espèce également, le motif d'exception de l'article 9.2, g) du RGPD, à savoir l'intérêt public prépondérant, constitue la base sur laquelle le traitement des données biométriques est justifié. Cette exception n'implique évidemment pas que l'accès à l'ensemble du réseau et du système d'information d'une installation portuaire puisse être soumis à la vérification des données biométriques. Seuls les modules susceptibles de faire l'objet d'abus peuvent être soumis à cette obligation."

[25] Extrait de l'Exposé des motifs : "*Les personnes qui savent où se trouve la cargaison criminelle peuvent l'isoler pour la récupérer ultérieurement. Le conducteur d'un chariot cavalier dans un terminal à conteneurs est un exemple d'employé qui, avec de mauvaises intentions ou sous la contrainte, peut tout simplement placer la cargaison à un endroit convenu à l'avance. Ces personnes sont activement approchées, avec ou sans recours à la force ou aux menaces, pour fournir une assistance aux bandes criminelles. Le renforcement du contrôle de ces activités rendra non seulement plus difficile la possibilité d'activités criminelles, mais protégera également les employés de l'installation portuaire. L'utilisation de la biométrie dans la manutention des marchandises peut garantir que ces chariots cavaliers ne peuvent être mis en marche qu'après vérification de l'identité du conducteur.*"

matière, l'Autorité demande de spécifier explicitement dans le projet que si l'exploitant d'une installation portuaire veut prévoir le traitement de données biométriques, tous les éléments concrets à cet égard doivent être repris dans l'évaluation de la sûreté (voir également le point 51).

53. Tout comme pour l'installation et l'utilisation de caméras de surveillance intelligentes, le traitement de données biométriques à grande échelle en vue de l'identification unique des personnes concernées est soumis à une analyse d'impact relative à la protection des données obligatoire. L'Exposé des motifs précise que celle-ci doit être reprise dans l'évaluation de la sûreté. L'Autorité en prend acte.

54. Sur la base de l'évaluation de la sûreté, un plan de sûreté qui doit être soumis à l'approbation de l'ANSM est élaboré. Seuls les traitements de données biométriques qui sont officiellement approuvés par l'ANSM seront effectivement autorisés. À cet effet, l'Exposé des motifs spécifie qu'il doit ressortir explicitement des plans de sûreté à quelle personne concernée le traitement de données biométriques s'applique et pour quelles parties de l'installation portuaire. Les auteurs du projet estiment que l'obligation de faire approuver le plan de sûreté par une autorité publique offre une protection supplémentaire contre les abus des possibilités proposées dans cet article.

Article 2.5.2.85 (Reconnaissance du sous-traitant des données biométriques)

55. Afin d'être reconnue comme sous-traitant de données biométriques conformément à la disposition du projet, l'entreprise doit être établie dans l'Espace économique européen, avoir une unité d'établissement en Belgique et se soumettre à un audit réalisé par la Cellule de sûreté maritime et le Contrôle de la navigation, en collaboration avec le Centre pour la Cybersécurité. Dans ce cadre, on vérifiera que l'entreprise respecte les normes ISO requises ou les normes déclarées équivalentes conformément à la réglementation relative à la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Il sera également vérifié que le système de traitement biométrique qu'ils ont développé répond aux trois exigences suivantes[26] :

- "*1° lors de la collecte initiale des données biométriques d'un individu, les caractéristiques individuelles et uniques des données brutes doivent être converties en informations codées, après quoi les données brutes sont immédiatement effacées*" (**meilleure formulation** : 1° lors de la première phase de collecte des données biométriques, les caractéristiques uniques et individuelles de l'individu sont codées et enregistrées en tant que gabarit, après quoi les données biométriques brutes sont immédiatement supprimées) ;

[26] L'Autorité propose un certain nombre d'adaptations du texte afin d'améliorer la lisibilité de l'article.

- "*2° lors de la vérification de l'identité de l'individu, il est seulement vérifié si les données collectées au cours du processus de vérification correspondent aux données stockées lors de la collecte initiale*[27]" (**meilleure formulation** : 2° lors de la vérification de l'identité de l'individu, il est seulement vérifié si les informations collectées au moment où l'individu souhaite s'authentifier correspondent au gabarit qui a été enregistré lors de la première phase de collecte) ;
- "*3° le stockage des informations codées est uniquement conservé sur un support de stockage durable qui est conservé par l'individu et aucun stockage sur les bases de données du sous-traitant n'est autorisé*" (**meilleure formulation** : 3° le gabarit est exclusivement conservé sur un support de stockage durable en possession de l'individu, aucun stockage n'étant autorisé dans les bases de données du sous-traitant).

56. En la matière, l'Autorité constate que les auteurs du projet optent pour un système biométrique qui, conformément à la recommandation n° 01/2021 de l'Autorité, offre la plupart des garanties contre les abus et limite autant que possible l'ingérence dans les droits et libertés des personnes concernées. Par souci d'exhaustivité, l'Autorité demande encore de spécifier dans le projet que les données biométriques collectées lors de la deuxième phase de collecte (le point 2° ci-dessus) ne peuvent pas non plus être conservées plus longtemps que nécessaire pour comparer ces données collectées au gabarit. De cette manière, à aucun moment des données biométriques (tant des données brutes que des gabarits) ne sont conservées dans les systèmes (centraux) du sous-traitant. Les seules données qui peuvent être conservées sont les fichiers de journalisation (par exemple : nom, lieu, heure) du contrôle d'accès biométrique.

57. Après la reconnaissance de l'entreprise, un audit de suivi est systématiquement réalisé dans la période comprise entre vingt-quatre et trente-six mois après un audit précédent. L'Autorité en prend acte.

58. En conclusion, moyennant le respect toutefois des remarques formulées dans le présent avis et des autres lignes directrices qui découlent de la recommandation n° 01/2021, l'Autorité estime que le cadre légal défini par le projet pour le traitement de données biométriques peut offrir suffisamment de garanties concernant la protection des données à caractère personnel.

---

[27] Une erreur s'est glissée dans l'explication de cet article dans l'Exposé des motifs : "*lors de la vérification de l'identité de la personne, aucune comparaison ne peut être effectuée avec une base de données biométriques. Il est uniquement permis de comparer le modèle stocké des données biométriques avec les informations* ***contenues sur le support de données que la personne porte sur elle***.**"**

Il est par contre correct d'indiquer qu'il est seulement autorisé de comparer le gabarit - stocké sur un support durable en possession de la personne concernée (par exemple un badge d'accès) - avec les informations que l'individu présente au système lors de la deuxième phase de collecte (chaque fois que l'individu souhaite s'authentifier). Pour des explications détaillées à ce sujet, l'Autorité renvoie à la section 2.3 *Le processus de traitement biométrique* de sa recommandation n° 01/2021.

Article 2.5.2.86 (Finalités, généralités)

59. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel ne peut être effectué que pour des finalités déterminées, explicites et légitimes.

60. Outre les finalités concrètes identifiées dans le cadre du traitement de données biométriques (points 49 – 54) (et dans une moindre mesure de l'utilisation de caméras de surveillance (intelligentes) (points 39 – 48)), cet article définit de manière plus générale les finalités pour le traitement de données à caractère personnel conformément au chapitre 2 du titre 5 du livre 2 du Code belge de la Navigation :

- *"1° garantir la sûreté maritime dans les ports et les installations portuaires ;*
- *2° prévenir les actions illicites ;*
- *3° détecter, poursuivre et sanctionner les actions illicites ;*
- *4° garantir la sûreté des personnes travaillant dans les ports et les installations portuaires ;*
- *5° réaliser les tâches des services de renseignement ;*
- *6° vérifier le respect de l'interdiction imposée conformément à l'article 4, § 3bis, de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes ou à l'article 4.1.2.48 du Code belge de la Navigation ;*
- *7° vérifier le respect de l'interdiction imposée aux personnes qui, en vertu du chapitre X de la loi du 20 juillet 1990 relative à la détention préventive, ont reçu la condition de ne pas se rendre dans un port ou une installation portuaire."*

61. En ce qui concerne le point 2°, l'Autorité réitère ses remarques relatives à la notion d' 'actions illicites', conformément au point 17.

62. Quant aux points 3° et 5°, l'Autorité souligne que détecter, poursuivre et sanctionner les actions illicites et réaliser les tâches des services de renseignement ne sont pas des finalités qui sont poursuivies en tant que telles par les responsables du traitement identifiés à l'article 2.5.2.91. À la lumière de la finalité centrale du projet, à savoir garantir la sûreté des ports et des navires, il semble recommandé d'isoler les finalités susmentionnées et de spécifier que les traitements dans ce cadre sont effectués par les autorités compétentes (services de police, autorités judiciaires et services de renseignement) conformément à la réglementation qui leur est applicable. En outre, vu que les traitements réalisés par ces acteurs ne relèvent pas du champ d'application du RGPD, l'Autorité a aussi soumis le projet pour avis à l'Organe de contrôle de l'information policière (le COC) et au Comité permanent de contrôle des services de renseignements et de sécurité

(le Comité R), en application du principe du guichet unique conformément à l'article 54/1 de la LCA.

63. Les points 6° et 7° prévoient que les données des personnes interdites de port peuvent être traitées en vue du contrôle obligatoire du respect de l'interdiction de port, conformément à l'article 2.5.2.81 (voir les points 36 – 37).

64. Par souci d'exhaustivité, l'Autorité demande d'identifier également une finalité dans cet article concernant la formation (requise) de certains acteurs (voir les points 27 – 28). En effet, comme cela a déjà été expliqué précédemment, l'organisation de telles formations (et examens) donne lieu à un traitement de données à caractère personnel des candidats concernés. Toutefois, cela n'empêche pas que la détermination des modalités de ce traitement puisse être déléguée au Roi.

65. Enfin, le deuxième alinéa de cet article stipule que "*Les données des membres des services d'inspection*[28] *sont traitées en vue d'identifier l'auteur d'un rapport d'inspection ou d'un procès-verbal*". Cette disposition a été reprise suite à une remarque du Conseil d'État dans son avis 69.362/1 sur un projet d'arrêté royal *optimisant les dispositions relatives au travail maritime*[29].

66. Moyennant la prise en considération des remarques conformément aux points 61, 62 et 64, l'Autorité estime que les traitements de données à caractère personnel envisagés sont effectués pour des finalités déterminées, explicites et légitimes.

Articles 2.5.2.87 - 2.5.2.88 (Catégories de personnes concernées et de données à caractère personnel)

67. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de 'minimisation des données').

68. Les articles 2.5.2.87 et 2.5.2.88 définissent respectivement les personnes physiques concernées et les catégories de données à caractère personnel à traiter.

69. Pour les visiteurs des installations portuaires (dont les travailleurs et les membres de la direction) et les membres du personnel chargés de la manutention de la cargaison :

"*1° les nom et prénoms ;*

2° le numéro de registre national pour les Belges ;

[28] Tels que visés à l'article 4.2.4.4.

[29] Pour des explications complémentaires, voir l'Exposé des motifs (p. 68 - 69).

3° les date de naissance et adresse pour les non-Belges ;
4° le numéro de carte d'identité ou de passeport ;
5° les données biométriques, le cas échéant, conformément à l'article 2.5.2.84 ;
6° l'objectif de la visite ;
7° les heures d'arrivée et de départ et la date de la visite ;
8° la plaque d'immatriculation des voitures entrant et sortant des installations portuaires ;
9° la photo ;
10° l'adresse e-mail."

70. Tout d'abord, bien que l'Autorité reconnaisse l'importance d'une identification correcte et du traitement de données y afférent répondant aux exigences de qualité et d'exactitude, elle souligne que l'utilisation du numéro de Registre national en Belgique est strictement réglementée par l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physiques* (ci-après : la loi du 8 août 1983). L'utilisation du numéro de Registre national n'est pas permise sans autorisation préalable, soit par le ministre de l'Intérieur, soit par ou en vertu d'une loi, d'un décret ou d'une ordonnance. En outre, à la lumière de l'article 87 du RGPD, il faut veiller à ce que l'utilisation du numéro de Registre national soit limitée aux cas dans lesquels elle est strictement nécessaire et où des mesures techniques et organisationnelles encadrent adéquatement l'utilisation sécurisée.

71. L'Autorité attire l'attention sur le fait que ni la formulation de l'article 2.5.2.88, ni celle de l'article 2.5.2.89 ne constitue une autorisation explicite au sens de l'article 8 de la loi du 8 août 1983.

72. Concernant le traitement du numéro de carte d'identité ou de passeport, l'Autorité se demande quelle est la plus-value de cette donnée par rapport aux autres catégories de données à caractère personnel à traiter. La durée de validité de ces documents et donc des numéros qui y sont liés est limitée dans le temps. En cas de perte, vol ou détérioration, ce numéro sera déjà devenu obsolète avant l'expiration de la durée de validité normale. De plus, l'Autorité attire l'attention sur l'obligation, dans le chef des responsables du traitement, de veiller à l'exactitude des données et de les tenir à jour, si nécessaire, conformément à l'article 5.1.d) du RGPD. À défaut d'une plus-value démontrable, cette information doit être supprimée.

73. Le traitement (les modalités du traitement) de données biométriques a (ont) déjà été commenté(es) en détail aux points 49 – 58 du présent avis.

74. Pour les conditions en matière d'utilisation de caméras intelligentes pour la reconnaissance des plaques d'immatriculation, l'Autorité renvoie aux points 42 – 44 du présent avis.

75. À la lumière des finalités poursuivies, les autres catégories de données à caractère personnel ne donnent lieu à aucune remarque particulière[30].

76. Pour les PSO (agents de sûreté portuaire[31]), PFSO, CSO et SSO, les données suivantes sont traitées :

"*1° les nom et prénoms ;*
2° le numéro de registre national pour les Belges ;
3° les date de naissance et adresse pour les non-Belges ;
4° l'adresse e-mail ;
5° le résultat de l'examen pour les PFSO ;
6° la photo."

77. En ce qui concerne l'utilisation du numéro de Registre national, l'Autorité renvoie à sa remarque exprimée au point 70. Pour le reste, l'Autorité ne formule aucune remarque particulière.

78. Pour les inspecteurs, les données suivantes peuvent être traitées :

"*1° les nom et prénoms ;*
2° le numéro d'identification donné par le service public pour lequel l'inspecteur travaille ;
3° la photo."

79. Afin d'accroître la cohérence du texte, l'Autorité demande de remplacer le terme '*inspecteurs*' à l'article 2.5.88, § 3 par '*membres des services d'inspection visés à l'article 4.2.4.4*', conformément à l'article 2.5.2.87 Pour le reste, il n'y a pas de remarque concernant les données à caractère personnel à traiter.

80. Enfin, "pour les personnes qui se sont vu imposer une interdiction conformément à l'article 4, § 3*bis* de la Loi relative aux drogues ou à l'article 4.1.2.48 du Code belge de la Navigation et les personnes qui, en vertu du chapitre X de la loi du 20 juillet 1990 *relative à la détention préventive*, se sont vu imposer la condition de ne pas se rendre dans un port ou une installation portuaire, les données suivantes peuvent être traitées :

"*1° les nom et prénoms ;*
2° le numéro de registre national pour les Belges[32] ;
3° la date jusqu'à laquelle l'interdiction est en vigueur ;

[30] En la matière, l'Exposé des motifs précise encore que le traitement des photographies est nécessaire pour la création de badges d'accès et d'identification. L'adresse e-mail est utilisée pour la communication avec les personnes concernées.

[31] Voir la note de bas de page n° 4.

[32] Voir à nouveau le point 700.

4° les ports et installations portuaires où l'interdiction est en vigueur."

81. L'Autorité en prend acte.

Article 2.5.2.89 (Accès)

82. Cet article prévoit : "*Les membres de l'ANSM, du CLSM concerné, de la Cellule de la sûreté maritime, du ministère public, des services de renseignement et des services d'inspection visés à l'article 4.2.4.4 ont accès aux données visées à l'article 2.5.2.**~~84~~ 88** et aux fins visées à l'article 2.5.2.**~~82~~ 86***[33].
Par dérogation à l'alinéa 1er, seuls le responsable du traitement, le sous-traitant et les services de renseignement et la police fédérale et locale ont accès aux données biométriques." L'Exposé des motifs ajoute à cela qu'il s'agit d'une énumération exhaustive des services publics qui sont chargés de contrôler et de vérifier le respect de la réglementation en matière de surveillance maritime.

83. Comme cela a déjà été expliqué ci-dessus (voir les points 33 – 35), il est nécessaire que les modalités de l'accès aux données à caractère personnel soient mieux alignées sur la réglementation relative à la plate-forme ISPS via lequel cet accès aura probablement lieu.

84. En outre, l'Autorité se demande à quelles données biométriques les services de renseignement et la police fédérale et locale peuvent accéder. En effet, comme il découle de l'article 2.5.2.85 - et comme l'exige également l'Autorité -, les données biométriques brutes doivent immédiatement, lors de la première phase de collecte, être converties en un gabarit codé qui n'est conservé que sur un support de stockage durable en possession exclusive de la personne concernée. Bien que l'Autorité reconnaisse logiquement que ces données seront traitées par le responsable du traitement et les sous-traitants en vue de l'organisation et de la gestion du contrôle d'accès biométrique, elle souligne que dans ce contexte, seules les données suivantes peuvent être conservées :
    - les données de journalisation du contrôle d'accès biométrique (sans que celles-ci puissent contenir des données biométriques) ;
    - le gabarit biométrique en possession exclusive de la personne concernée (par exemple le badge d'accès ou d'identification).

    Compte tenu de ce qui précède, l'Autorité estime que le passage susmentionné ne présente aucune plus-value (et crée de surcroît la confusion) et doit dès lors être supprimé.

[33] Au point 34, il a déjà été fait référence aux renvois fautifs dans le projet.

85. L'Autorité souligne que le gabarit ne peut sous aucun prétexte être copié, ni conservé en dehors du support de stockage durable (sauf bien sûr pendant la vérification effective de l'identité de la personne concernée lors d'un contrôle d'accès, moyennant la prise en considération de la remarque formulée au point 56).

Article 2.5.2.90 (Délai de conservation)

86. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

87. À cet effet, l'article 2.5.2.90 précise ce qui suit : "*Les données visées à l'article 2.5.2.88 sont conservées pendant la période déterminée dans le plan de sûreté et ne peuvent jamais excéder une période de* ***10 ans****.*
Par dérogation à l'alinéa 1er, les données biométriques ne peuvent être conservées que pendant un délai de 2 ans après la visite d'une installation portuaire ou après que l'intéressé n'a plus accès aux réseaux ou systèmes d'information.
Par dérogation à l'alinéa 1er, ***les données des personnes visées à l'article 2.5.2.87, 4° et 5°****, sont immédiatement effacées après l'expiration ou la levée de l'interdiction de port."*

88. Concernant le délai de conservation 'standard' de 10 ans, l'Exposé des motifs spécifie qu'un tel délai est nécessaire dans le cadre de l'application des règlements, incluant les procédures judiciaires. L'Autorité en prend acte mais demande à l'ANSM de vérifier, lors de l'approbation des plans de sûreté, que l'application du délai de conservation susmentionné soit toujours justifiée. Lorsqu'il s'avère que pour certaines données, un délai plus court peut être appliqué, il faut agir en conséquence.

89. Ensuite, l'article 2.5.2.90 prévoit un délai de conservation particulier pour les données biométriques des personnes concernées. Comme cela a déjà été expliqué ci-dessus, les données biométriques brutes doivent immédiatement, lors de la première phase de collecte, être effacées après avoir été converties en un gabarit biométrique codé. L'Autorité a également demandé dans ce cadre de spécifier que les données de la deuxième phase de collecte (la vérification effective) ne pouvaient pas non plus être conservées plus longtemps que le temps nécessaire à leur comparaison avec le gabarit[34]. Une donnée biométrique (le gabarit) n'est conservée que sur le badge d'accès, qui est uniquement en possession de la personne concernée.

[34] Voir le point 56.

90. L'Autorité s'interroge dès lors sur le délai de conservation prévu de deux ans maximum après qu'une personne déterminée a eu accès pour la dernière fois aux locaux physiques ou après qu'elle n'a plus accès aux réseaux et systèmes d'information. Un tel délai ne peut en effet pas être appliqué lorsque la personne concernée ne remet pas son badge d'accès. L'Autorité demande par contre de spécifier dans le projet que les badges (sur lesquels un gabarit biométrique a été enregistré) soient, si possible, immédiatement détruits après que les personnes concernées n'ont plus accès aux locaux physiques visés ou aux réseaux et systèmes d'information. Si la destruction du badge n'était pas possible pour l'une ou l'autre raison, il faut au moins prévoir la possibilité de 'désactiver' ce badge afin d'en rendre l'utilisation ultérieure impossible. À ce moment, cette personne doit quoi qu'il en soit être supprimée de la liste des personnes ayant accès aux locaux susmentionnés (ce afin d'éviter qu'une personne qui prétend faussement avoir perdu son badge puisse encore y accéder). Cela n'affecte évidemment en rien le délai de conservation standard qui peut s'appliquer vis-à-vis des données de journalisation du contrôle d'accès biométrique.

91. Une deuxième exception concerne les données des personnes qui se sont vu imposer une interdiction de port. L'Autorité prend acte du fait que ces données sont immédiatement supprimées à l'issue de l'interdiction de port. À cette fin, il est possible de travailler à l'aide d'un système automatisé qui supprime les données dès que l'échéance est atteinte.

Article 2.5.2.91 (Responsable du traitement)

92. Conformément à l'article 4.7) du RGPD, le responsable du traitement est toute personne physique ou morale, autorité publique, tout service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. L'Autorité rappelle en outre que la désignation du responsable du traitement ou la qualification en tant que tel doit être adéquate au regard des circonstances factuelles. En d'autres termes, pour chaque traitement de données à caractère personnel, il faut vérifier qui poursuit effectivement les finalités et qui contrôle effectivement le traitement[35].

93. L'article 2.5.2.91 dispose que :
"Le PFSO est le responsable du traitement pour les visiteurs d'une installation portuaire[36]*.*
L'ANSM est le responsable du traitement pour le PSO, le PFSO, le CSO, le SSO et les inspecteurs.
L'ANSM est le responsable du traitement pour les personnes visées à l'article 2.5.2.87, 4° et 5°."

[35] Voir également en la matière les lignes directrices 07/2020 de l'EDPB *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*. Consultables via le lien suivant : https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_fr.pdf.

[36] Les particularités relatives au sous-traitant des données biométriques ont déjà été abordées aux points **Error! Reference source not found.** et suivants.

94. Tout d'abord, l'Autorité demande de toujours reprendre dans cet article, par analogie avec l'article 2.5.2.90, la précision suivante : 'Le/l' … est le responsable du traitement pour les données des/ du … visées à l'article 2.5.2.88, § … qui sont traitées pour les finalités visées à l'article 2.5.2.86'.

95. Ensuite, l'Autorité fait remarquer que le PFSO est désigné en tant que responsable du traitement pour les données des visiteurs (dont les membres du personnel et les administrateurs) d'une installation portuaire. Il en résulte que l'entreprise où le PFSO a été engagé (l'exploitant de l'installation portuaire) intervient uniquement en tant que sous-traitant au sens de l'article 4.8) du RGPD. Les articles 5.1.f) et 24 du RGPD obligent le responsable du traitement à prendre les mesures techniques et organisationnelles appropriées nécessaires afin de garantir un niveau de sécurité adapté au risque d'abus. En outre, l'article 28.1 du RGPD exige que le responsable du traitement fasse uniquement appel à des sous-traitants qui présentent des garanties suffisantes de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée.

96. En la matière, l'Autorité doute toutefois que le PFSO, qui, le cas échéant, est un travailleur ou un administrateur de l'exploitant de l'installation portuaire, intervienne effectivement en tant que responsable du traitement. En effet, le PFSO ne choisit pas quelle entreprise peut exploiter l'installation portuaire et il semble peu plausible qu'il détermine lui-même les finalités, et plus important encore, les moyens du traitement. En outre, cela impliquerait qu'à la moindre violation du RGPD, le PFSO peut être tenu personnellement responsable, ce qui, en particulier si le PFSO est un travailleur de l'exploitant, ne saurait se justifier. Dès lors, l'Autorité estime que les exploitants des installations portuaires doivent être qualifiés de responsables du traitement. Cela n'affecte en rien l'obligation de désigner un PFSO conformément aux dispositions du projet. Le PFSO peut être désigné au sein de l'entreprise en tant que point de contact central en matière de protection des données.

97. La désignation de l'ANSM en tant que responsable du traitement pour le PSO, le PFSO, le CSO, le SSO et les inspecteurs ne donne lieu à aucune remarque particulière en matière de protection des données à caractère personnel.

98. Enfin, l'Exposé des motifs précise qu'en ce qui concerne les personnes frappées d'une interdiction de port, la responsabilité de l'ANSM se limite à la vérification de l'interdiction. Le traitement proprement dit des décisions, jugements ou arrêts qui imposent une telle interdiction de port continue à relever du champ d'action du SPF Justice. L'Autorité en prend acte.

Articles 2.5.2.92 – 2.5.2.95 (Limitation des droits)

99. Les articles précités prévoient une dérogation au droit à l'information, au droit d'accès, au droit de rectification et au droit à la limitation du traitement en ce qui concerne les traitements qui ont pour objectif la préparation, l'organisation, la gestion et le suivi des enquêtes effectuées, y compris les enquêtes judiciaires et l'application éventuelle d'une sanction administrative.

100. Toute limitation des droits des personnes concernées en vertu du RGPD doit non seulement poursuivre un des objectifs énoncés à l'article 23.1 du RGPD mais également satisfaire aux formes prescrites à l'article 23.2 du RGPD[37]. En outre, toute limitation des droits des personnes concernées doit rester limitée à ce qui est strictement nécessaire, tant en ce qui concerne la portée que la durée[38]. Bien que l'Autorité comprenne que pour des traitements de contrôle et d'inspection, l'on puisse prévoir des dérogations à certains droits garantis par le RGPD (afin de ne pas compromettre les contrôles et les enquêtes menées), elle estime que la formulation actuelle des articles soumis pour avis n'est pas compatible avec les conditions conformément à l'article 23 du RGPD et aux exigences en matière de sécurité juridique et de prévisibilité dans le chef des personnes concernées[39].

101. Tout d'abord, les responsables du traitement qui bénéficient de ces dérogations doivent être explicitement mentionnés dans le projet.

102. Ensuite, l'Autorité souligne que conformément à l'article 23.2 du RGPD, il incombe aux auteurs du projet de spécifier la portée des limitations, non seulement au niveau des droits auxquels il est dérogé mais également au niveau des limites des limitations visées. À cet égard, l'Autorité recommande, sans vouloir être exhaustive, de spécifier que les dérogations aux droits des personnes concernées s'appliquent uniquement pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête (incluant les actes préparatoires

---

[37] Voir dans ce cadre les lignes directrices de l'EDPB "*Guidelines 10/2020 on restrictions under Article 23 GDPR*" (actuellement, uniquement disponible en anglais). Consultables via le lien suivant : https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf.

[38] Voir également plusieurs avis de l'Autorité : l'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,* plus précisément les considérants 36 à 38 ; l'avis n° 41/2018 du 23 mai 2018 *concernant un avant-projet de loi portant des dispositions financières diverses* et l'avis n° 88/2018 du 26 septembre 2018 sur un *projet d'arrêté du Gouvernement flamand portant adaptation des arrêtés du Gouvernement flamand au 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 (règlement général sur la protection des données ou RGPD).*

[39] Lignes directrices de l'EDPB "*Guidelines 10/2020 on restrictions under Article 23 GDPR* ", p. 8 : "*the domestic law must be sufficiently clear in its terms to give individuals an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such restrictions.*"

jusqu'à maximum un an à partir de la réception de la demande d'exercice du droit[40]) et pendant la période nécessaire pour les poursuites en cours, dans la mesure où l'exercice des droits porterait préjudice aux besoins du contrôle, de l'enquête ou des actes préparatoires.

103. Enfin, afin que les articles susmentionnés du projet soient compatibles avec l'article 23.2 du RGPD, il faut en outre prévoir des garanties similaires à celles prévues dans le chapitre 5/1 du *Code pénal social*. Ces dérogations et garanties pour les droits et libertés des personnes concernées ont en effet déjà été approuvées par l'Autorité dans son avis n° 34/2018[41]. On pense ici à : désigner les fondements factuels ou juridiques sur lesquels la décision de refus de l'exercice d'un droit de la personne concernée s'est basée, informer les personnes concernées du rejet de leur demande et des motifs y afférents, à moins que cela ne compromette l'objectif du contrôle, informer les personnes concernées qui ont voulu exercer leurs droits de la levée de la dérogation après clôture du contrôle, informer les personnes concernées des voies de recours dont elles disposent à cet égard, ...

c. Article 21 du projet

104. L'article 21 du projet complète le livre 4 du Code belge de la Navigation par un titre 6 libellé comme suit : "*Dispositions particulières pour la mer du Nord*". Il s'agit d'un régime *lex specialis* à l'égard de l'installation de caméras de surveillance en mer du Nord par des personnes privées et des autorités publiques étant donné que la Loi caméras ne peut pas s'appliquer ici[42]. Néanmoins, les auteurs du projet ont opté pour un cadre conceptuel[43] et une structure conformes à la loi susmentionnée, ce qui favorise la transparence et la prévisibilité de la réglementation.

105. Les dispositions de ce titre s'appliquent à l'installation et à l'utilisation de caméras dans la mer territoriale belge et la Zone Économique Exclusive pour les finalités suivantes[44] :

"1° la prévention, la constatation ou la détection des délits contre les personnes et les marchandises ;

2° la protection du milieu marin ;

3° la recherche scientifique ;

4° la garantie de la sécurité de la navigation ;

---

[40] Afin de garantir une limitation raisonnable dans le temps pour la dérogation.

[41] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/avis-n-34-2018.pdf.

[42] Plusieurs conditions posées par la Loi caméras n'ont en effet aucun sens dans ce contexte : l'autorisation requise par la commune, l'installation de pictogrammes et la clôture au moyen d'une enceinte physique de domaines privés pour pouvoir installer des caméras à des fins privées, ...

[43] Par analogie avec l'article 2 de la Loi caméras, l'article 4.6.1.2 utilise les mêmes définitions pour les notions de caméra, caméra fixe ou mobile et caméra intelligente.

[44] Article 4.6.1.4.

5° la garantie de la sûreté des ouvrages de construction et de génie civil, des câbles et des pipelines ;
6° la garantie de la sûreté des zones maritimes belges ;
7° la conservation des ressources vivantes."

À l'exception des remarques formulées ci-dessous, l'Autorité estime que ces finalités sont déterminées, explicites et légitimes.

Article 4.6.1.6 (Utilisation de caméras fixes dans la mer territoriale)

106. "*L'initiative d'installer une ou plusieurs caméras fixes* - caméras placées dans un lieu fixe au cours de l'observation afin de filmer à partir de cet emplacement - *est prise par le responsable du traitement, qui ne peut être qu'une autorité publique*". À cet effet, le responsable du traitement adresse la demande d'installation d'une caméra fixe à la Cellule de la sûreté maritime et précise les points suivants :

"*1° l'emplacement de l'installation de la caméra ;*
2° le périmètre ;
3° la finalité de l'utilisation de la caméra ;
4° les spécifications de la caméra ;
5° le délai de conservation proposé, qui ne peut excéder la durée maximale telle que déterminée ***au paragraphe 5, alinéa 2***[45] *;*
6° la manière dont les données sont traitées."

La Cellule de la sûreté maritime transmet le dossier avec l'avis du Carrefour de l'information maritime[46] (ci-après : le MIK) au ministre en charge de la mobilité maritime qui décide de l'installation et des modalités des caméras. Une fois les caméras installées, la Cellule de la sûreté maritime annonce leur installation via un Avis aux Navigateurs et une publication sur son site web.

107. L'Exposé des motifs précise que cette décision ministérielle remplace l'autorisation par la commune qui est requise pour l'installation de caméras sur la terre ferme[47]. La publication des données de la caméra dans les publications nautiques bien connues remplace le pictogramme qui doit être placé en application de la Loi caméras afin de signaler l'existence d'une surveillance par caméra.

[45] L'Autorité constate qu'il n'y a pas d'article 4.6.1.6, § 5, deuxième alinéa. L'Autorité suppose qu'il faut faire référence au § 7.

[46] Le Carrefour de l'information maritime, tel que visé à l'article 3, 7° de l'Accord de coopération entre État fédéral et la Région flamande *concernant la création d'une structure de garde côtière et la coopération au sein de celle-ci* du 8 juillet 2005, se compose de quatre partenaires, à savoir la défense, la police maritime, l'Administration générale des Douanes et Accises et la DG Navigation.

[47] Article 5 de la Loi caméras.

108. Concernant la procédure de demande susmentionnée, l'Autorité formule les remarques suivantes :

- il semble incontestablement recommandé de prévoir un formulaire de demande standardisé. La forme et le contenu de celui-ci peuvent le cas échéant être déterminés par le Roi[48]. En particulier, les notions de '*spécifications de la caméra*' et de '*manière dont les données sont traitées*' laissent une trop grande marge d'interprétation subjective ;
- le projet ne régit nulle part les modalités de l'obligation d'avis impliquée dans le chef du MIK, ceci doit être rectifié. Si cette obligation découle d'une autre disposition légale, il faut y faire référence ;
- par analogie avec les articles 2.5.2.19 et 2.5.2.35, il faut prévoir une durée de validité maximale pour l'approbation par le ministre, après quoi une nouvelle demande doit être introduite.

109. Le paragraphe 4 de cet article dispose ce qui suit : "*Le responsable du traitement tient un registre des activités de traitement d'images des caméras effectuées sous sa responsabilité. Le Roi détermine le contenu de ce registre, ses modalités et son délai de conservation*." En la matière, l'Autorité se demande quel est le rapport entre ce registre et le registre des activités de traitement que le responsable du traitement doit déjà tenir conformément à l'article 30 du RGPD[49]. Une précision en ce sens peut par exemple être reprise dans l'Exposé des motifs. Quoi qu'il en soit, l'Autorité souligne qu'en ce qui concerne le contenu du registre, le Roi ne peut pas porter préjudice aux exigences minimales exposées à l'article 30 du RGPD[50].

110. Le paragraphe 5 établit que "*La visualisation de ces images en temps réel n'est autorisée que par les services visés à l'article 4.2.4.4/1*", à savoir le Contrôle de la navigation, la Cellule de la sûreté maritime, les membres de l'ANSM, l'Administration générale des Douanes et Accises, le Ministère de la Défense, la police fédérale et l'Unité de Gestion du modèle mathématique de la Mer du Nord. Par analogie avec les dispositions de la Loi caméras concernant la visualisation en temps réel des images de caméras de surveillance, il faut spécifier dans le projet qu'un tel accès n'est admis que dans le but de permettre aux services compétents d'intervenir immédiatement en cas d'infraction ou de dommage et de guider au mieux ces services dans leur intervention dans le cadre de leur mission légale, ou dans le but de réunir la preuve de faits constitutifs d'infraction ou générateurs de dommages, de rechercher et d'identifier les auteurs des faits, les témoins ou les

[48] Par analogie avec le formulaire qui doit être transmis par le responsable du traitement aux services de police conformément à la Loi caméras.

[49] Que le responsable du traitement en question occupe ou non plus ou moins de 250 personnes, l'Autorité estime que les traitements de données à caractère personnel visés comportent un risque pour les droits et libertés des personnes concernées.

[50] La même remarque s'applique aux dispositions similaires dans la Loi caméras. Voir également à cet égard le point 23 de l'avis n° 53/2017 de la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité (voir la note de bas de page n° 15).

victimes. Si les auteurs du projet identifient des finalités complémentaires pour la visualisation des images en temps réel (par exemple dans le cadre de la recherche scientifique), cela doit être explicitement repris dans le projet.

111. Ensuite, le paragraphe 6 précise : *"L'enregistrement des images n'est autorisé qu'afin de recueillir des preuves de faits constitutifs d'un délit ou causant des dommages et détecter et identifier les auteurs, témoins ou les victimes."* L'Autorité estime que cette disposition donne à tort l'impression que les caméras qui sont installées conformément à ce chapitre peuvent uniquement être utilisées pour recueillir des preuves de faits constitutifs d'un délit ou causant des dommages et pour détecter et identifier les auteurs, témoins ou victimes. Dans le cas où le responsable du traitement a indiqué[51] une autre finalité pour l'installation de caméras conformément à l'article 4.6.1.4 (par exemple la recherche scientifique), il doit également être possible d'enregistrer et d'analyser les images. En outre, l'Autorité souligne qu'il faut faire une distinction entre les images de caméras qui doivent être qualifiées ou non de données à caractère personnel. En effet, s'il ne s'agit pas d'un traitement de données à caractère personnel, les dispositions du RGPD ne doivent logiquement pas être respectées. Dès lors, l'Autorité demande que cette disposition soit adaptée comme suit : 'L'enregistrement des images **qui donnent lieu à un traitement de données à caractère personnel** n'est autorisé que **pour la réalisation des objectifs visés à l'article 4.6.1.4**.'

112. La même remarque s'applique en ce qui concerne le délai de conservation des images conformément au paragraphe 7 : "*Si ces images ne peuvent contribuer à prouver un délit, un dommage ou une nuisance, ou à identifier un auteur, un perturbateur de l'ordre public, un témoin ou une victime, elles ne sont pas conservées plus de six mois.*" Tout d'abord, il semble recommandé de spécifier que seules les images qui doivent être qualifiées de données à caractère personnel sont soumises à un délai de conservation. En outre, on ne tient à nouveau pas compte des autres finalités qui peuvent être poursuivies licitement au moyen de ces caméras. Enfin, et incidemment, l'Autorité ne voit pas clairement à quel moment il est établi que les images ne peuvent contribuer à prouver un délit, un dommage ou une nuisance, ou à identifier les personnes visées, de sorte que le 'délai de conservation' de six mois commence à courir. L'Autorité demande donc d'adapter le paragraphe 7 comme suit : 'Les images **qui donnent lieu à un traitement de données à caractère personnel** ne sont pas conservées plus longtemps que ce qui est strictement nécessaire pour la réalisation des objectifs tels que visés à l'article 4.6.1.4, sans que ce délai puisse dépasser … années.' Il appartient aux auteurs du projet ou aux responsables du traitement de définir un délai de conservation maximal approprié en fonction de la finalité poursuivie.

[51] La finalité de l'installation des caméras doit également être explicitement définie lors de la demande ET dans le registre des activités de traitement.

113. Enfin, le paragraphe 8 précise que par dérogation au principe que seules les autorités publiques peuvent intervenir en tant que responsable du traitement, l'exploitant d'un ouvrage de construction ou de génie civil, d'un câble ou d'un pipeline peut également introduire une demande d'installation de caméras de surveillance dans la mer territoriale, à condition que :
"1° l'utilisation des caméras figure dans le plan de sûreté visé à l'article 2.5.2.64 ; ou
2° l'utilisation de la caméra a pour objectif le respect de la zone de sécurité établie conformément à l'arrêté royal du 4 février 2020 établissant des zones de sécurité dans les espaces marins sous la juridiction de la Belgique."

Dans ce cas, les paragraphes 2 - 4 et 6 - 7 de l'article 4.6.1.6 s'appliquent *mutatis mutandis*. L'Autorité en prend acte.

Articles 4.6.1.7 – 4.6.1.8 (Caméras mobiles dans la mer territoriale/caméras dans la Zone Économique Exclusive)

114. Les articles 4.6.1.7 et 4.6.1.8 établissent respectivement que des caméras mobiles ne peuvent être installées dans la mer territoriale que par une autorité visée à l'article 4.1.4.4/1 conformément aux modalités à l'article 4.6.1.6 et que l'utilisation de caméras fixes ou mobiles dans la Zone Économique Exclusive est autorisée conformément à la réglementation qui s'applique à la mer territoriale, à condition que le demandeur (qui souhaite installer les caméras) puisse démontrer que la caméra est utilisée pour l'un des droits visés à l'article 56[52] ou 60[53] de la Convention des Nations Unies sur le droit de la mer. L'Autorité en prend acte et renvoie au commentaire de l'article 4.6.1.6.

Article 4.6.1.9 (Utilisation cachée de caméras)

115. Conformément à cet article, l'utilisation cachée (lisez : sans autorisation préalable des personnes concernées) de caméras est interdite. Le fait de pénétrer dans un lieu indiqué conformément à l'article 4.6.1.6, § 3, vaut comme autorisation préalable. Tant la formulation que le fondement de cet article sont particulièrement problématiques. Tout d'abord, l'Autorité souligne

[52] Cet article dispose que dans la zone économique exclusive, l'État côtier a : "*a) des droits souverains aux fins d'exploration et d'exploitation, de conservation et de gestion des ressources naturelles, biologiques ou non biologiques, des eaux surjacentes aux fonds marins, des fonds marins et de leur sous-sol, ainsi qu'en ce qui concerne d'autres activités tendant à l'exploration et à l'exploitation de la zone à des fins économiques, telles que la production d'énergie à partir de l'eau, des courants et des vents ; b) juridiction, conformément aux dispositions pertinentes de la Convention, en ce qui concerne, i) la mise en place et l'utilisation d'îles artificielles, d'installations et d'ouvrages, ii) la recherche scientifique marine, iii) la protection et la préservation du milieu marin ; c) les autres droits et obligations prévus par la Convention.*"

[53] Cet article concerne le droit exclusif de l'État côtier de procéder à la construction et d'autoriser et réglementer la construction, l'exploitation et l'utilisation : "a*) d'îles artificielles ; b) d'installations et d'ouvrages affectés aux fins prévues à l'article 56 ou à d'autres fins économiques; d'installations et d'ouvrages pouvant entraver l'exercice des droits de l'État côtier dans la zone.*"

que 'le fait de pénétrer dans un tel lieu' ne peut en aucun cas générer un consentement valable au sens du RGPD[54]. Par ailleurs, l'Autorité souligne que le consentement en tant que base juridique pour le traitement n'est (ne peut) quoi qu'il en soit pas (être) invoqué ici. Les traitements de données à caractère personnel initiés par ces caméras reposent en effet sur l'article 6.1.e) du RGPD (l'intérêt public). Il est dès lors préférable de préciser que 'toute installation (toute utilisation) de caméras dans la mer territoriale ou dans la zone économique exclusive contraire aux dispositions des articles 4.6.1.4 et 4.6.1.6 - 4.6.1.8 est interdite'. L'Autorité demande de modifier l'article adéquatement en ce sens.

Article 4.6.1.10 (Caméras intelligentes)

116. Étant donné qu'il ne transparaît nulle part pour quelles raisons les images de caméra sont nécessaires pour la reconnaissance automatique des navires - en effet, comme indiqué par le demandeur, la reconnaissance automatique se fait via un AIS-transponder (ondes radio) -, l'Autorité réitère ses remarques conformément aux points 45 – 46. Si un navire ne dispose pas, à tort, d'un AIS-transponder, des caméras de surveillance ordinaires peuvent suffire pour filmer le navire et le cas échéant filmer toute infraction. L'article doit être supprimé.

Article 4.6.1.11 (Non-discrimination)

117. Cet article dispose : "*Les caméras ne peuvent ni fournir des images qui portent atteinte à l'intimité d'une personne, ni viser à recueillir des informations relatives aux opinions philosophiques, religieuses, politiques ou syndicales, à l'origine ethnique ou sociale, à la vie sexuelle ou à l'état de santé.*" Il découle également de l'Exposé des motifs que cette disposition a été tirée de la Loi caméras et doit être interprétée par analogie.

118. L'Autorité doute toutefois de la plus-value de cet article. En effet, comme cela a déjà été expliqué au point 115, l'utilisation de caméras de surveillance contraire aux articles 4.6.1.4 et 4.6.1.6 - 4.6.1.8 est considérée comme interdite. Aucune finalité telle que définie à l'article 4.6.1.4 ne justifie l'utilisation de caméras qui produiraient des images au sens de cet article. En outre, l'Autorité rappelle que conformément à l'article 9.1 du RGPD, tout traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que tout traitement des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits, à moins qu'il n'existe un motif d'exception conformément à

[54] Article 4.11) du RGPD : " *"consentement" de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement*".

l'article 9.2 du RGPD. Vu que cette disposition répète donc purement et simplement la réglementation déjà en vigueur[55], l'Autorité demande de supprimer cet article.

Article 4.6.1.12 (Droit d'accès)

119. Cet article prévoit ce qui suit : "*Toute personne filmée a un droit d'accès aux images.*
La personne filmée adresse à cet effet une demande au responsable du traitement. Cette demande comporte des indications suffisamment détaillées pour permettre de localiser les images concernées de manière précise.
Lorsque la personne filmée peut prétendre au droit d'obtenir une copie conformément à l'article 15, 3, du RGPD, le responsable du traitement peut répondre à la demande d'accès en faisant visionner à la personne filmée les images où elle apparaît, sans lui fournir une copie des images, afin de garantir que :
1° les droits et libertés d'autrui, comme prévu à l'article 15, 4, du RGPD, ne sont pas compromis ;
2° la sécurité publique ou la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, en application de l'article 23, paragraphe 1er, c) et d), du RGPD, ne sont pas compromises." [Ndt : il convient de supprimer le passage "ou l'exécution de sanctions pénales" de la version française du projet]

120. L'article précité vise donc à prévoir une limitation du droit de la personne filmée d'obtenir une copie des images lorsque cela porte atteinte aux droits et libertés d'autrui ou lorsque la sécurité publique ou la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière sont compromises. Tout d'abord, l'Autorité constate que le point 1° constitue une violation de l'interdiction de retranscription du RGPD[56]. Cette disposition doit être supprimée. De plus, l'Autorité se demande s'il n'est pas opportun, par analogie avec les articles 2.5.2.92 - 2.5.2.95, de prévoir une limitation plus large des droits des personnes concernées en ce qui concerne les traitements de données réalisés à l'aide de caméras qui ont pour objectif la préparation, l'organisation, la gestion et le suivi des enquêtes effectuées, y compris les enquêtes judiciaires et l'application éventuelle d'une sanction administrative. En tout cas, il va de soi que les remarques de l'Autorité conformément aux points 100 – 103 s'appliquent *mutatis mutandis* à l'égard de ces limitations. Cet article doit être modifié adéquatement en ce sens.

[55] Ce qui implique d'ailleurs une violation de l'interdiction de retranscription de règlements européens ; l'applicabilité directe des règlements européens implique une interdiction de transposer ceux-ci en droit national car un tel procédé "*peut créer une équivoque en ce qui concerne tant la nature juridique des dispositions applicables que le moment de leur entrée en vigueur*". Voir dans ce cadre : CJUE, 7 février 1973, Commission c. Italie (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Voir également : CJUE, 10 octobre 1973, Fratelli Variola S.p.A. c. Service des impôts italien (C-34/73), Recueil de jurisprudence, 1973, p. 981, § 11 ; CJUE, 31 janvier 1978, Ratelli Zerbone Snc c. Amministrazione delle finanze dello Stato, Recueil de jurisprudence (C-94/77), 1978, p. 99, §§ 24-26.

[56] Conformément à l'article 15.4 du RGPD, le droit d'obtenir une copie est déjà limité s'il porte atteinte aux droits et libertés d'autrui.

PAR CES MOTIFS,
l'Autorité

estime que les modifications suivantes s'imposent dans le projet :

- préciser la notion d' 'action illicite' (points 17 – 26) ;
- préciser quels acteurs assurent concrètement la réalisation de quelles finalités de la plate-forme ISPS, y compris les traitements de données à caractère personnel dans ce cadre (points 33 – 35, 38 et 83) ;
- améliorer la formulation de la finalité en matière d'interdiction de port de la plate-forme ISPS (point 37) ;
- clarifier la problématique en matière d'utilisation de caméras intelligentes pour la reconnaissance des plaques d'immatriculation dans la mesure où les acteurs concernés n'ont pas accès aux données des plaques d'immatriculation dans le répertoire des véhicules (point 43) ;
- supprimer les dispositions en matière d'utilisation de caméras intelligentes pour la reconnaissance automatique des navires (points 45 – 46 et 116) ;
- spécifier explicitement toutes les finalités pour lesquelles des caméras intelligentes peuvent, le cas échéant, être utilisées (points 47 – 48) ;
- supprimer les inexactitudes dans l'Exposé des motifs concernant un délai de tolérance d'1 an pour supprimer progressivement l'utilisation des données biométriques ou pour inciter le législateur à prévoir un cadre juridique (point 49) ;
- spécifier toutes les finalités pour le traitement de données biométriques à l'article 2.5.2.84, § 1er (point 51) ;
- adapter les formulations en matière d'exigences pour un système biométrique (points 55 –-56) ;
- spécifier une finalité pour le traitement de données à caractère personnel dans le cadre de la formation obligatoire de certains acteurs (points 27 – 28 et 64) ;
- prévoir une autorisation pour l'utilisation du numéro de Registre national dans le chef des acteurs concernés (points 70 – 71, 77 et 80) ;
- supprimer l'information 'numéro de carte d'identité ou de passeport' à l'article 2.5.2.88 (point 72);
- supprimer le passage relatif à l'accès aux données biométriques pour les services de renseignement et la police fédérale et locale à l'article 2.5.2.89 (point 84) ;
- revoir le délai de conservation (maximal) qui s'applique à l'égard des données biométriques (points 89 – 90) ;

- réexaminer la désignation du PFSO en tant que responsable du traitement pour les visiteurs d'une installation portuaire (points 94 – 96) ;
- reformuler les dispositions relatives à la limitation des droits des personnes concernées (points 100 – 103 et 120) ;
- mettre en œuvre les modifications/compléments envisagé(e)s concernant la procédure de demande pour l'installation de caméras dans la mer du Nord (point 108) ;
- par analogie avec la Loi caméras, reprendre des garanties complémentaires concernant la visualisation en temps réel des images (point 110) ;
- reformuler les dispositions concernant les exigences pour l'enregistrement d'images et le délai de conservation maximal de ces images (points 111 – 112) ;
- modifier l'article 4.6.1.9 relatif à l'interdiction de filmer en cachette de manière à ce qu'il corresponde mieux à la réalité (point 115) ;
- supprimer l'article 4.6.1.11 en matière de non-discrimination (point 118).

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