Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n°114/2023 du 18 juillet 2023

Objet: Demande d'avis concernant un projet de loi modifiant la loi du 15 mai 2007 relative à la sécurité civile en vue de régler l'utilisation de caméras par les services opérationnels de la sécurité civile (CO-A-2023-197)

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et 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 « LCA »);

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

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

Vu la demande d'avis de Madame Annelies Verlinden, Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique (ci-après « la demanderesse »), reçue le 12 mai 2023;

Émet, le 18 juillet 2023, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. La demanderesse a sollicité l'avis de l'Autorité concernant un projet de loi modifiant la loi du 15 mai 2007 relative à la sécurité civile en vue de régler l'utilisation de caméras par les services opérationnels de la sécurité civile (ci-après « le projet »).

2. Le projet, annoncé par la circulaire du 20 janvier 2023[1], entend permettre aux zones de secours, au Service d'Incendie et d'Aide Médicale Urgente bruxellois (SIAMU) et aux unités opérationnelles de la Protection civile, de collecter des données à caractère personnel à l'aide de caméras, le cas échéant intelligentes voire capables de traiter des données biométriques et de traitées ces données à des fins opérationnelles, probatoires, didactiques ou pédagogiques, dans les lieux fermés non accessibles au public dont ils sont les gestionnaires ainsi que sur les lieux de leurs interventions.

3. Pour ce faire, le projet insère un nouveau chapitre dans la loi relative à la sécurité civile du 15 mai 2007 s'inspirant de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance[2] (ci-après « loi caméras ») et de la loi sur la fonction de police (ci-après « LFP »), mais généralement sans mentionner une référence aux longs développements figurant dans les travaux parlementaires de ces normes (et des normes modificatives), qui sont pourtant indispensables à la compréhension des concepts utilisés.

4. Il ressort de l'exposé des motifs du projet que l'adoption de cette *lex specialis* permettra d'exclure les caméras des services opérationnels de la sécurité civile[3] du champ d'application de la loi caméras, car « *ces services souhaitent pouvoir utiliser différents types de caméras à des fins autres que la seule surveillance* ». L'exposé précise en effet que « *la pratique montre les difficultés d'application de cette loi générale aux missions spécifiques des services opérationnels de la sécurité civile, notamment en ce qui concerne l'utilisation de caméras mobiles* ». L'Autorité constate toutefois que les difficultés rencontrées dans la pratique ne sont pas mentionnées dans l'exposé des motifs du projet.

5. En revanche, l'Autorité constate que la version actuelle des dispositions de la loi caméras définissant le champ d'application de la loi et permettant l'adoption de législations particulières[4], résulte d'une

[1] Circulaire de la Ministre de l'Intérieur relative à la violence à l'égard du personnel opérationnel des zones de secours (MB 20.02.2023) qui remplace la circulaire du 30 septembre 2021 ayant le même objet et adoptée suite à la multiplication des agressions envers les pompiers (voy. https://www.sudinfo.be/art/850634/article/2021-10-13/slfp-pompiers-une-hausse-inquietante-des-agressions-envers-les-pompiers)

[2] MB 31.05.2007

[3] A savoir les zones de secours, le Service d'Incendie et d'Aide Médicale Urgente bruxellois (SIAMU) et les unités opérationnelles de la Protection civile

[4] A savoir les art. 2 et 3 de la loi

modification par la loi du 21 mars 2018[5]. Comme le précise le commentaire de l'art. 63 de cette loi : jusqu'alors, la définition de la notion de « *caméra de surveillance* » impliquait des finalités qui ne s'appliquaient qu'aux seuls services de police[6]. Depuis lors, le déplacement des dispositions relatives à l'utilisation des caméras de surveillance par les services de police, dans la LFP, a conduit au remplacement de cette définition par des termes plus généraux, « *à savoir que les caméras de surveillance sont des systèmes d'observation dont le but est la surveillance et le contrôle des lieux* » pour des finalités précisées dans le commentaire de l'art. 64, à savoir « *d'une part,* (…) *de prévenir, constater ou déceler des infractions contre les personnes ou les biens; d'autre part,* (…) *de prévenir, constater, 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* »[7]. Le commentaire précise en outre que « *la division des finalités en deux points a pour objectif de mettre en évidence le fait que la prévention, la constatation ou la recherche d'incivilités, le contrôle du respect des règlements communaux et le maintien de l'ordre public ne sont pas de la compétence de tous, mais uniquement des instances à qui cette compétence est confiée par la loi* »[8].

6. En ce qui concerne l'application de législations particulières, le commentaire précise que « *l'objectif n'était certainement pas de permettre d'éluder l'application de la loi caméras, dès qu'un texte légal ou réglementaire faisait mention de l'utilisation de caméras* (…) » et que « *la seule mention de l'utilisation de caméras de surveillance dans une autre loi n'empêche donc pas l'application de la loi caméras, dès lors que les finalités d'installation et d'utilisation sont celles visées à l'article 3* [de la loi caméras] »[9]. Enfin, le commentaire de l'art. 65 précise que la loi caméras contient une règle de conflit de lois (art. 3/1) de sorte « *qu'en cas de surveillance par caméras pour plusieurs finalités dont une de celles prévues par l'article 3 de la loi caméras, par un même responsable du traitement, les différentes législations s'appliquent de manière simultanée et qu'en cas de conflit entre celles-ci, les règles de la loi caméras prévalent* »[10].

7. L'art. 3 du présent projet exclut la finalité de contrôle du travail du personnel de son champ d'application. L'art. 4 définit les concepts utilisés. L'art. 5 régit l'utilisation de caméras en fonction du type de lieu où les enregistrements sont pris. L'art. 6 permet l'enregistrement du son par les caméras mobiles et fixes temporaires (et prévoit, pour se faire, une exception à l'interdiction de l'interception

---

[5] « *Modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière* » (MB 16.04.2018)

[6] « *Prévenir, constater ou déceler les délits contre les personnes ou les biens ou les nuisances au sens de l'article 135 de la nouvelle loi communale, ou maintenir l'ordre public* », voy. Doc. parl. Ch., 54-2855/001, 4 javier 2018, session 2017-2018, p. 59 et sv. (https://www.lachambre.be/FLWB/PDF/54/2855/54K2855001.pdf)

[7] *Ibidem*, p. 62

[8] *Ibidem*, p. 63

[9] *Ibidem*, p. 64

[10] *Ibidem*, pp. 65-66

des communications électroniques prévue à l'art. 259*bis* du Code pénal). Il en résulte une incertitude quant à la volonté du législateur d'avoir recours à des bodycams[11]. L'art. 7 décrit les finalités justifiant l'utilisation de caméras par les services opérationnels de la sécurité civile, énonce les finalités pour lesquelles des traitements ultérieurs sont possibles, le cas échéant après anonymisation « *si la finalité poursuivie le permet* », autorise l'utilisation de caméras biométriques et interdit l'utilisation des caméras visées par le projet pour évaluer individuellement le personnel ou pour initier une procédure disciplinaire. Le commentaire de l'art. 7 précise que la zone d'intervention - à savoir le périmètre dans lequel des données peuvent être collectées par une caméra pour des finalités liées à l'évaluation ou à la surveillance - est définie comme la « *zone délimitée par le directeur du poste de commandement opérationnel en fonction d'une situation concrète d'urgence et dans laquelle les actions nécessaires sont mises en œuvre pour gérer ladite situation* »[12]. L'art. 8 prévoit une approbation préalable et unique du conseil de zone (pour la zone de secours) ou du ministre ou de son délégué (pour les unités opérationnelles de la protection civile) pour l'utilisation de caméras. Le même article prévoit que l'autorisation d'utiliser des caméras doit être rendue publique « *au minimum* » via une publication sur le site du service concerné. L'art. 9 prévoit une durée de conservation maximale d'un mois, mais porte cette durée à 12 mois « *lorsque les images et les sons sont utilisés dans le cadre d'un retour d'expérience* ». L'art. 10 permet le visionnage des images et l'écoute du son en temps réel ou pendant l'incident, mais limite cette faculté à certaines catégories de personnes (membres d'un service opérationnel ou non) désignées dans chaque service opérationnel de la sécurité civile par le commandant de zone ou le chef d'unité. Le même article prévoit également la possibilité pour les services opérationnels de la sécurité civile de recevoir en temps réel ou pendant ou après un incident, des images et des sons pris par d'autres autorités, services ou intervenants, mais également par des tiers (tels que des « *spectateurs* »). L'art. 11 prévoit que les images enregistrées seront accessibles aux personnes compétentes au sein des services opérationnels, désignés par le commandant de la zone ou le chef d'unité, pour autant que l'accès à ces données soit nécessaire et proportionné. Le même article prévoit également une journalisation des accès. L'accès à des personnes extérieurs est également autorisé. L'art. 12 fait référence au secret professionnel ou au devoir de discrétion des personnes ayant accès aux images et sons. Le même article indique qu'il est interdit de partager, avec la presse ou via les médias sociaux, des images et sons par lesquels des personnes ou des données à caractère personnel peuvent être identifiées, à moins que les images et les sons ne soient rendues anonymes ou que toutes les personnes filmées ou photographiées n'aient donné leur consentement au partage des images et des sons. L'art. 13 concerne les transferts de données. L'art. 14 désigne le SPF Intérieur comme responsable des traitements effectués par les unités opérationnelles de la protection civile et les zones de secours elles-mêmes pour les traitements que ces dernières effectuent. Le même article désigne en outre le commandant de zone pour la zone de secours et le Président du Comité de direction du Service public fédéral Intérieur pour la Protection civile, comme responsables

[11] Raison pour laquelle, ce point sera abordé *in fine*

[12] Par référence à l'art. 38 de l'AR du 22 mai 2019 relatif à la planification d'urgence

opérationnels du traitement, définit comme « *la personne qui décide de l'objectif du traitement et des moyens utilisés pour y parvenir* ». La même disposition met la réalisation d'un DPIA à charge de ces responsables opérationnels. L'art. 15 met la tenue d'un registre des activités de traitement à charge des responsables opérationnels. L'art. 16 concerne la mise en œuvre de l'obligation de transparence par l'affichage du pictogramme prévu par l'arrêté royal du 10 février 2008 ainsi que par la publication d'un avis sur le site des services opérationnels concernés. L'art. 17 modalise le droit d'accès des personnes concernées et prévoit des limitations à l'exercice de ce droit. Enfin, l'art. 19 introduit une sanction pénale à l'encontre de toute personne qui enfreint les dispositions déterminant les objectifs d'utilisation des caméras ou les dispositions déterminant les destinataires possibles des données enregistrées ainsi que pour toute personne qui détient une image obtenue en violation de ces dispositions.

8. La note au Conseil des Ministres, qui accompagne le projet, précise que le projet s'inspire des avis de l'Autorité et de l'Organe de contrôle de l'information policière. L'Autorité attire l'attention de la demanderesse sur l'adoption par l'EDPB, de lignes directrices sur le traitement des données à caractère personnel par des dispositifs vidéo[13].

II. EXAMEN DU PROJET

1. Prévisibilité, effectivité et importance de l'ingérence

9. L'Autorité constate que les dispositions du projet, dans la mesure où elles prévoient des traitements de données à caractère personnel, touchent *de facto* aux droits et libertés fondamentaux, dont la Constitution confie particulièrement la garantie au législateur. Or, conformément à l'article 8 de la Convention européenne des droits de l'homme, l'article 22 de la Constitution ainsi que l'article 6.3 du RGPD, lu à la lumière du considérant 41 du RGPD, toute norme prévoyant un traitement de données à caractère personnel (et donc une ingérence dans les droits et libertés des personnes concernées) doit être **claire et précise**. En outre, son **application doit être prévisible** pour les personnes concernées. Il en va d'autant plus ainsi lorsque l'ingérence revêt un caractère particulièrement important, comme c'est le cas en l'espèce[14].

[13] Lignes directrices 3/2019 adoptées le 29 janvier 2020 (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf)

[14] L'EDPB rappelle à cet égard que « l'utilisation intensive de dispositifs vidéo a une incidence sur le comportement des citoyens. La mise en œuvre généralisée de ces outils dans de nombreux domaines de la vie des particuliers exercera une pression supplémentaire sur ceux-ci aux fins de la détection des anomalies éventuelles. En effet, ces technologies peuvent restreindre les possibilités de mouvement anonyme et d'utilisation anonyme des services et limitent généralement la possibilité de passer inaperçu. Les incidences en matière de protection des données sont énormes » (*op. cit.*, point 1)

10. En l'espèce, comme le relevait déjà le rapport de la commission de l'Intérieur du Sénat en 2006[15], la vidéosurveillance dans les lieux publics requiert « *une base légale claire et une approche intégrée* », en d'autres termes, un cadre légal général. Dans la mesure où tout régime d'exception a pour effet de compliquer l'appréhension, par la personne concernée, des hypothèses dans lesquelles le législateur autorise une ingérence dans ses droits et libertés par le traitement de ses données, un tel régime doit être évité dans toute la mesure du possible. A noter que le régime distinct applicable aux services de police se justifie par le fait que le traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, relève du Titre II LTD transposant la directive (UE) 2016/680. Cependant, c'est bien le droit commun de la protection des données (et en particulier le RGPD) qui s'applique à l'ensemble des services opérationnels de la sécurité civile.

11. L'Autorité estime par conséquent que, sauf à démontrer à l'aide d'éléments objectifs, l'impossibilité d'adapter les règles générales de la lois caméras aux besoins des services opérationnels de la sécurité civile[16], il y a lieu d'appliquer la lois caméras aux caméras utilisés par ces services à des fins de surveillance de l'espace public. L'Autorité estime cependant que, même si pour certaines finalités, le besoin d'une législation particulière est susceptible être démontré, **l'installation et l'utilisation de caméras à des fins de prévention des vols dans les lieux dont les services opérationnels de la sécurité civile sont responsables du traitement, ne justifie en aucun cas un régime d'exception** par rapport n'importe quelle autre autorité, école, hôpital, banque, etc…

12. Toutefois, l'utilisation de caméras par ces services à des fins autres que la surveillance peut, pour autant que les dispositions du RGPD ne soient pas suffisantes à cet égard, être encadrée par une loi particulière (conformément aux art. 6.1.c) ou 6.1.e) du RGPD). L'Autorité rappelle au passage qu'en vertu du principe de minimisation des données[17], dans certaines situations évoquées dans l'exposé des motifs (tels que la surveillance de reprise de feu) seule l'utilisation de caméras ne permettant pas[18] le traitement de données à caractère personnel (telles que des caméras thermiques dans un périmètre interdit d'accès, précisément en raison du danger de reprise d'incendie) sera permise. Les règles d'utilisation de caméras dans ces circonstances échapperaient bien entendu au contrôle de l'Autorité.

---

[15] Doc. parl. Sénat, 3-1413/1, 18 avril 2006 (https://www.senate.be/www/?MIval=index_senate&MENUID=25400&LANG=fr)

[16] Le commentaire des art. 2 et 3 du projet précise que le projet permettra de ne plus avoir à déclarer les caméras des services de sécurité civile aux autorités policières. Or, les travaux préparatoires de la loi de 2018 modifiant la LFP et la loi caméras dispose que « *pour des raisons opérationnelles, il reste utile pour les services de police de savoir où sont placées des caméras de surveillance. C'est pourquoi seule cette déclaration est maintenue dans la loi caméras* », voy. Doc. parl. Ch., 54-2855/001, 4 janvier 2018, session 2017-2018, p. 70 ; Il en résulte qu'une absence de déclaration aux services de police ne s'appliquera durablement qu'à la condition de dûment justifier en quoi les raisons opérationnelles invoquées ne seraient pas l'application en l'espèce.

[17] Voy. *infra*

[18] Techniquement et/ou en raison des conditions de leur utilisation

Dans le même ordre d'idées, le repérage de corps sans vie ou d'objets, n'impliquent pas de traitement de données à caractère personnel et peuvent donc intervenir avec des moyens techniques autres que des caméras de surveillance au sens de la loi caméras.

13. L'adaptation éventuelle de la loi caméras (ou, d'une loi particulière) est l'occasion pour l'Autorité d'attirer l'attention de la demanderesse sur le fait que, comme le rappelle un récent rapport au Haut-Commissaire des Nations-Unies aux Droits humains, s'inquiétant des menaces que la surveillance fait peser sur les démocraties : « *les Etats négligent trop souvent de démontrer l'efficacité des systèmes de surveillance qu'ils mettent en œuvre* »[19]. Par conséquent, afin d'éviter qu'à l'avenir il puisse être reproché à la Belgique de ne pas démontrer l'efficacité des systèmes de surveillance qu'elle met en œuvre, l'Autorité estime qu'il convient de prévoir par une disposition du projet (rendue applicable à la loi caméras également) que des statistiques seront réalisées par chaque responsable du traitement des données collectées par des caméras placées sur l'espace public, aux **fins de la publication d'un rapport d'évaluation** (selon une périodicité à déterminer dans le projet, mais qui ne devrait pas être inférieure à tous les 3 ans) portant sur l'efficacité de chacune des caméras de surveillance déjà installées, par rapport aux finalités pour lesquelles leur placement a été considéré comme justifié[20].

2. Finalités

14. En vertu de l'article 5.1.b) du RGPD, un traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes.

15. En vertu de l'art. 7 du projet, les services opérationnels de sécurité civile peuvent utiliser des caméras, dans le cadre de leurs missions[21], pour :

1° obtenir un aperçu de la zone d'intervention et la cartographier, évaluer la situation et suivre l'évolution de l'incident pour en assurer sa gestion ;

2° surveiller la zone d'intervention ou certains lieux présentant un risque particulier de manière préventive[22] ;

---

[19] Rapport du 4 août 2022, The right to privacy in the digital age, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement, point 54

[20] Pour un exemple de disposition répondant adéquatement à cette exigence d'efficacité, voy. l'art. 151c de la Loi communale néerlandaise (https://wetten.overheid.nl/BWBR0005416/2017-07-01/#TiteldeelIII_HoofdstukIX_Artikel151c)

[21] Qui, en vertu de l'art. 11 de la loi relative à la sécurité civile sont :

1° le sauvetage de personnes et l'assistance aux personnes dans des circonstances dangereuses et la protection de leurs biens;

2° l'aide médicale urgente telle que définie à l'article 1er de la loi du 8 juillet 1964 relative à l'aide médicale urgente;

3° la lutte contre l'incendie et l'explosion et leurs conséquences;

4° la lutte contre la pollution et contre la libération de substances dangereuses en ce compris les substances radioactives et les rayons ionisants; et

5° l'appui logistique.

[22] Le commentaire relatif à cette disposition précise qu'il s'agit de « *surveiller d'une part, la zone d'intervention, pour empêcher tout accès non autorisé à la zone et éviter que la situation ne s'aggrave et surveiller d'autre part, d'autres lieux présentant un*

3°repérer des objets, des corps ou des incidents[23];

4° protéger le personnel et les biens du service[24] ;

5° prendre des images et/ou du son dans le cadre de la planification d'urgence[25] et de la gestion de situations d'urgence[26], telles que réglées par l'arrêté royal relatif à la planification d'urgence.

16. Sous réserve d'une adaptation permettant le maintien de l'application de la loi caméras, au minimum à l'installation et à l'utilisation de caméras à des fins de prévention des vols dans les lieux dont les services opérationnels de la sécurité civile sont responsables du traitement, l'Autorité considère que ces finalités respectent l'art. 5.1.b) du RGPD.

17. L'art. 7, §2 du projet limite le traitement ultérieur « *des images et du son* » aux finalités suivantes :

1° évaluer une intervention[27] ;

2° disposer de preuves en cas de litige devant les tribunaux administratifs ou judiciaires compétents[28];

3° disposer d'archives visuelles et sonores, conformément à l'article 89 du RGPD ;

4° à des fins didactiques et pédagogiques dans le cadre de la formation des membres des service opérationnels de la sécurité civile, après anonymisation conformément au RGPD ;

5° pour sensibiliser et informer la population après anonymisation conformément au RGPD.

18. Le projet s'abstient d'utiliser la notion de « *caméra de surveillance* » (contrairement à la loi caméras[29]). Il en résulte que les finalités liées à la surveillance et le contrôle des lieux aux fins de prévenir, constater ou déceler des infractions contre les personnes ou les biens doivent être omises du projet dans la

risque particulier de manière préventive. Par exemple, il serait possible de surveiller à distance si un incendie qui a été éteint se rallume ou de surveiller un lieu qui présente un risque d'incendie »

[23] *Par exemple, une caméra équipée d'une certaine technologie peut distinguer la forme d'une épave de voiture ou d'un corps humain (sans identifier la personne elle-même) ou encore détecter un soudain dégagement de fumée*

[24] *Par exemple, l'utilisation d'une caméra mobile pendant une intervention peut avoir une finalité probatoire pour tout délit. Les caméras fixes peuvent être utilisées, par exemple, pour détecter le vol d'équipements et protéger les biens du service. Ainsi, en cas de vol par un tiers ou par un pompier, la zone peut porter plainte et les images peuvent être envoyées à la police/justice. En revanche, les images ne pourront servir à une procédure en interne (procédure disciplinaire, suspension dans l'intérêt du service, évaluation, …) que si elles proviennent de caméras de surveillance du travail réglées par le règlement de travail.*

[25] A savoir : « *l'ensembles des mesures organisationnelles, procédurales et matérielles, et d'outils contribuant à la détermination des actions et mécanismes de coordination à mettre en place lors de la survenance d'une situation d'urgence, afin de pouvoir mobiliser dans les meilleurs délais les moyens humains et matériels nécessaires et ainsi organiser les interventions nécessaires à la protection de la population et des biens* »

[26] Cet AR définit ces situations comme « *tout événement qui entraîne ou qui est susceptible d'entraîner des conséquences dommageables pour la vie sociale, comme un trouble grave de la sécurité publique, une menace grave contre la vie ou la santé des personnes et/ou contre des intérêts matériels importants, et qui nécessite la coordination des acteurs compétents, en ce compris les disciplines, afin de faire disparaître la menace ou de limiter les conséquences néfastes de l'événement* »

[27] *Cette définition comprend à la fois l'évaluation interne par les services eux-mêmes et l'évaluation externe dans le cadre de la recherche (scientifique).*

[28] *Par exemple, lorsqu'un membre du personnel a été victime de violence et qu'il s'agit d'une affaire judiciaire, les images peuvent être utilisées comme preuves des faits.*

[29] Avant l'entrée en vigueur de la loi du 21 mars 2018, certaines des finalités reprises dans la définition ("*prévenir, constater ou déceler les délits contre les personnes ou les biens ou les nuisances au sens de l'article 135 de la nouvelle loi communale, ou maintenir l'ordre public*") s'appliquaient uniquement aux services de police et autres autorités publiques. Depuis lors, la loi caméras dispose que « *les caméras de surveillance sont des systèmes d'observation dont le but est la surveillance et le contrôle des lieux* »

mesure où une inapplicabilité de la loi caméras dans ce cas, n'est pas dûment justifiée. Dans ce cas, l'utilisation de caméras à d'autres fins pourra valablement être régie par le projet pour autant qu'il ne déroge pas au RGPD, dans les cas - supposément rares – où des données à caractère personnel seraient traités. Le cas échéant, l'Autorité estime qu'il conviendrait de prévoir que « *sans préjudice de l'application de la loi caméras, les données à caractère personnel collectées par les caméras installées et utilisées en vertu de la présente loi ne peuvent être traitées que pour autant que ce traitement soit nécessaire à l'exécution des missions d'intérêt public telles qu'énumérées à l'art. 11 de la loi relative à la sécurité civile* ». Ceci permettra en effet de prévoir une application stricte du principe de minimisation des données, à chaque fois que la loi caméras ne sera pas d'application.

19. Toutefois, si la demanderesse devait démontrer la nécessité de déroger à la loi caméras pour ces finalités, il y aurait lieu de mentionner que les caméras utilisées pour de telles finalités sont bien des caméras de surveillance. Par ailleurs le projet devra alors « *réellement comporter des règles, être suffisamment précis et donner suffisamment de garanties en ce qui concerne l'utilisation de caméras de surveillance* »[30].

20. Le commentaire relatif à l'art. 7, §3 précise que cette disposition du projet doit s'interpréter comme un rappel de l'interdiction du traitement des catégories particulières de données figurant à l'art. 9.1 du RGPD. Cependant, le libellé de cette disposition prête à confusion. Ce paragraphe prévoit en effet que les caméras peuvent pas « *viser à recueillir des informations relatives à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques,* [des données biométriques][31] *aux fins d'établir l'identité d'une personne physique ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ». L'Autorité rappelle à cet égard que l'interdiction prévue à l'art. 9.1. du RGPD ne concerne pas les finalités du traitement (ou un objectif de collecte), mais bien le traitement (quel qu'en soit l'objectif) de ces catégories particulières de données. L'Autorité estime par conséquent que la disposition et son commentaires doivent être clarifiés de manière à prévoir une interdiction du placement et de l'utilisation des caméras visées par le projet « *d'une manière qui prendre possible le traitement de catégories particulières de données au sens de l'art. 9 du RGPD* ». Ce faisant, il ne sera pas pour autant interdit d'utiliser des caméras lorsque cela s'avère nécessaire, par exemple en soutien d'une intervention dans un lieu de culte ravagé par les flammes (ne fut-ce qu'en application de l'exception prévue à l'art. 9.2.c) du RGPD). En revanche, lorsque les intérêts vitaux de personnes ne sont pas en jeu (ou ont cessé de l'être), cette formulation guidera le responsable du traitement quant à la manière de placer les caméras, quant à l'application du principe de minimisation et quant à l'interdiction de réutiliser les images (non anonymisées) à d'autres fins que la seule mission de secours.

[30] Doc. parl. Ch, 54-2855/001, *op. cit.*, p. 64

[31] Cette notion, figurant à l'art. 9.1. du RGPD, n'est pas mentionnée dans le projet

21. Enfin, l'art. 7, §4 du projet dispose que « *les caméras ne peuvent pas avoir pour objectif d'évaluer individuellement un membre du personnel ou de permettre la poursuite d'une procédure disciplinaire* », tout en relativisant cette affirmation dans le commentaire. L'Autorité estime que le commentaire relatif à cette disposition devrait permettre de comprendre clairement quels sont les traitements susceptibles d'être effectués à l'égard de données relatives à une infraction pénale, dont se serait rendu coupable un membre des services opérationnels de la sécurité civile ou un membre d'une autre autorité intervenante. A l'occasion de la reformulation de cette disposition, il conviendra également de préciser la manière dont cette disposition est appelée à coexister avec l'art. 29 C.I.Cr.[32] et l'art. 32 du Titre préliminaire du C.I.Cr.[33] lu en combinaison avec la condition de licéité des traitements figurant à l'art. 5.1.a) du RGPD. En effet, l'Autorité estime que l'effectivité du RGPD requiert de prévoir expressément qu'une preuve obtenue en méconnaissance du principe de finalité des traitements ne pourrait être valablement utilisée l'encontre de la personne concernée dans le cadre d'une procédure qui implique la prise d'une décision coercitive à son égard.

3. Proportionnalité/minimisation des données

22. 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").

Caméras intelligentes et « couplage »

23. L'art. 5 du projet prévoit le recours à de caméras intelligentes, définies à l'art. 4, 6° du projet comme des caméras comprenant « *des composants 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* ». Le commentaire de l'art. 4 se réfère utilement à l'exposé des motifs de la loi de 2018 modifiant la LFP précitée. Le commentaire cite également l'exemple des « *caméras de surveillance qui détectent les mouvements ou les bruits* ».

24. Le commentaire de l'art. 7 de la loi de 2018 précise qu'une « *caméra intelligente est celle qui, équipée d'une technologie supplémentaire, va pouvoir elle-même, au-delà du simple traitement d'images (collecte, enregistrement d'images), grâce au fait qu'elle est dotée de ou reliée à des détecteurs ou d'autres capteurs, traiter (filtrer, analyser) les images qu'elle recueille, de manière autonome ou non, en étant couplée ou non à des registres ou fichiers (caméra qui détecte des sons préenregistrés ou les mouvements, caméras ANPR, caméras de reconnaissance faciale, caméras reliées à des détecteurs qui*

[32] Obligation de dénonciation au Procureur du Roi des délits dont un fonctionnaire est le témoin

[33] Relatif à l'admissibilité des « preuves illicites » (dans la lignée de la jurisprudence Antigoon)

mesurent le poids et la hauteur, etc). Une bodycam qui enregistre l'image et le son, utilisée par un policier en intervention (qui prend donc part à la conversation qu'il enregistre), n'est donc pas une caméra intelligente, vu qu'elle ne filtre pas déjà les données au moment de la collecte ».

25. L'Autorité relève que le couplage dont il est question dans la loi de 2018 rend possible la mise en corrélation avec des listes de personnes, de véhicules, etc., au sens de l'art. 44/11/3decies, §4 LFP. Or, l'Autorité rappelle que toute ingérence dans le droit au respect de la protection des données à caractère personnel, n'est admissible que si elle est nécessaire et proportionnée à l'objectif (aux objectifs) qu'elle poursuit[34].

26. A cet égard, l'Autorité estime la transposition des dispositions d'une loi applicable aux services de police dans l'exercice de leurs missions de police administrative et judiciaire doit faire l'objet d'une justification en termes de nécessité et de proportionnalité, dans le commentaire de l'art. 5 du projet. Si la démonstration du caractère nécessaire et proportionné devait pouvoir être apportée, l'Autorité estime que **deux éléments importants** devront être pris en compte. Il s'agit **tout d'abord** du fait que l'exemple mentionné dans le commentaire de l'art. 4 du projet (la « *surveillance* » de mouvements ou de bruits), n'implique pas nécessairement un enregistrement des données. Cependant, si certains traitements de données collectées au moyens de caméras intelligentes devaient impliquer un enregistrement de données à caractère personnel (et qu'il était démontré qu'un tel enregistrement était nécessaire et proportionné), il y aurait lieu d'encadrer l'enregistrement de ces données (qui, contrairement à ce qui est prévu pour les services de police, devrait avoir lieu localement et non de manière centralisée) et le traitement des données enregistrées, sur le modèle de ce qui est prévu pour les banques de données techniques visées aux art. 44/11/3sexies LFP et sv. A noter que le dernier alinéa de l'art. 9 du projet[35] ne répond pas valablement à cette préoccupation et doit donc être reformulé. Le **second élément** important à prendre en compte est le fait qu'en ce qui concerne les

[34] un traitement de données à caractère personnel est considéré comme étant nécessaire s'il constitue la mesure la moins attentatoire pour atteindre l'objectif (d'intérêt général) qu'il poursuit. Il faut donc :

- Premièrement, que le traitement de données permette effectivement d'atteindre l'objectif poursuivi. Il faut donc démontrer, sur base d'éléments factuels et objectifs, l'efficacité du traitement de données à caractère personnel envisagé pour atteindre l'objectif recherché ;
- Deuxièmement, que ce traitement de données à caractère personnel constitue la mesure la moins intrusive au regard du droit à la protection de la vie privée. Cela signifie que s'il est possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel, le traitement de données initialement envisagé ne pourra pas être mis en place. Il faut, à cette fin, détailler et être en mesure de démontrer, à l'aide d'éléments de preuve factuels et objectifs, les raisons pour lesquelles les autres mesures moins intrusives ne sont pas suffisantes pour atteindre l'objectif recherché.

Si la nécessité du traitement de données à caractère personnel est démontrée, il faut encore démontrer que celui-ci est proportionné (au sens strict) à l'objectif qu'il poursuit, c'est-à-dire qu'il faut démontrer qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement. Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées. À nouveau, il faut être en mesure de démontrer que cette analyse a bien été réalisée avant la mise en œuvre du traitement.

[35] *Les images et les sons sont conservés par le responsable opérationnel du traitement sur un support de données qui est protégé conformément aux principes de protection des données dès la conception et de protection des données par défaut*

« *caméras de surveillances reliées à un fichier de données à caractère personnel, comme les caméras ANPR (avec reconnaissance automatique des plaques d'immatriculation) ou les caméras à reconnaissance faciale* (…), *il a été décidé* [par le législateur] *d'autoriser uniquement les caméras ANPR* ». A cet égard, l'Autorité prend acte de l'interdiction, prévue dans le projet, du recours à la reconnaissance faciale[36], mais estime que (sauf à en démontrer le caractère nécessaire et proportionné dans l'exposé des motifs du projet), le placement et l'utilisation de caméras intelligentes « *reliées à un fichier de données à caractère personnel* » devraient être expressément interdits par le projet.

Anonymisation et pseudonymisation

27. L'Autorité constate que les informations relatives à la stratégie d'anonymisation figurant dans le commentaire de l'art. 7 du projet ne sont pas satisfaisante[37]. En effet, ce libellé semble témoigner d'une confusion entre l'anonymisation et la pseudonymisation. Il y a donc lieu d'adapter le commentaire sur ce point.

28. L'Autorité réitère les considérations qu'elle exprime de manière constante dans ses avis, à savoir que l'identification d'une personne ne vise pas uniquement la possibilité de retrouver son nom et/ou son l'adresse mais également la possibilité de l'identifier par un processus d'individualisation, de corrélation ou d'inférence. Ainsi, le floutage du premier intervenant sur les lieux d'un incident ne permettra pas d'éviter efficacement une réidentification et les données ne pourront donc pas être considérées comme anonymes. En revanche, le floutage des images d'une foule pourraient être considérées comme atteignant le standard élevé de l'anonymisation.

29. L'Autorité attire l'attention du demandeur sur le fait qu'il existe une différence entre des données pseudonymisées définies par l'article 4(5) du RGPD comme des données *« qui ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires »* et des données anonymisées qui ne peuvent plus par aucun moyen raisonnable être attribuées à une personne précise et que seules ces dernières ne constituent plus des données personnelles et sont donc exclues du champs d'application du RGPD, conformément à son considérant 26 »[38].

---

[36] Qui se heurterait par ailleurs aux dispositions dispositions de la proposition de Règlement européen concernant l'intelligence artificielle (https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf) et à la jurisprudence de la Cour E.D.H. (voy. l'affaire Glukhin c. Russie du 4 juillet 2023 (https://hudoc.echr.coe.int/?i=001-225655))

[37] *L'anonymisation se fait conformément aux règles applicables à la protection de la vie privée, par exemple en rendant les visages ou les voix, les plaques d'immatriculation ou autres données à caractère personnel non identifiables*

[38] Pour plus d'informations, voir l'avis 5/2014 (WP216) relative aux techniques d'anonymisation, 2.2.3, p. 11 du Groupe 29, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

30. Dès lors, eu égard à la définition de donnée à caractère personnel telle que figurant à l'article 4, 1) du RGPD[39], il convient de s'assurer que le standard élevé requis pour l'anonymisation est bien atteint[40] et que les données ne sont pas simplement pseudonymisées. En effet, le traitement de données, même pseudonymisées, doit être considérée comme un traitement de données à caractère personnel au sens du RGPD.

31. Il résulte de ce qui précède que, si c'est bien de pseudonymisation (et non d'anonymisation) qu'il est question :
- il conviendra de se référer au rapport de l'Agence de l'Union européenne pour la cybersécurité relatif aux techniques et meilleures pratiques de pseudonymisation[41] ;
- et ce traitement devra être encadré par toutes les garanties requises et répondre aux principes prévalant en la matière[42].

Anonymisation et archivage

32. En ce qui concerne la finalité d'archivage, le commentaire de l'art. 7 précise que les images et le son doivent être anonymisés « *si la finalité poursuivie le permet* ». Ce libellé ne permet pas à une personne concernée de vérifier si c'est à bon droit que ces données n'ont pas fait l'objet d'une anonymisation en vue de l'archivage. L'Autorité attire l'attention de la demanderesse sur le fait que ce libellé est susceptible de résulter d'une confusion entre l'archivage prévu par la LFP (« *l'archivage informatique* » entre les mains du même responsable du traitement) et l'archivage au sens commun du terme. Dans la mesure où seul ce dernier s'applique en l'espèce, l'Autorité estime qu'il convient d'indiquer dans le projet que « *sans préjudice de la loi du 24 juin 1955 relative aux archives, un traitement ultérieur des images et du son aux fins d'archivage ne peut intervenir qu'après anonymisation des données à caractère personnel* ».

---

[39] A savoir : « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

[40] L'identification d'une personne ne vise pas uniquement la possibilité de retrouver son nom et/ou son l'adresse mais également la possibilité de l'identifier par un processus d'individualisation, de corrélation ou d'inférence.

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

[42] Il en va ainsi du principe de proportionnalité renvoyant à celui, plus spécifique, de « *minimisation* » des données impliquant que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard, des finalités pour lesquelles elles sont traitées, conformément à l'article 5, § 1er, c) du RGPD.

Communication de données par un « spectateur »

33. L'art. 10, §4 du projet permet aux services opérationnels de la sécurité civile de recevoir en temps réel ou pendant ou après un incident, des images et des sons « *pris par un tiers, par exemple un spectateur, qui contribuent à l'accomplissement de leurs missions légales, à condition que les images et les sons aient été pris conformément aux prescriptions légales* ».

34. L'Autorité attire l'attention sur le fait qu'une telle disposition ne doit pas être adoptée à la légère. Il y a tout d'abord lieu de préciser qu'un tel traitement de données peut déjà (sans être prévu par la loi) intervenir lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux d'une personne physique. (art. 6.1.d) du RGPD). Cependant, si le législateur décide de fonder cette communication sur une obligation légale (art. 6.1.c) du RGPD) ou l'exécution d'une mission d'intérêt public (art. 6.1.e) du RGPD), il y a lieu de déterminer les conditions de cette communication. En effet, le libellé actuel est susceptible d'être interprété comme permettant une communication de données à caractère personnel via une plateforme « *commerciale* »[43], utilisée à titre privé, par un préposé du responsable du traitement. Or, une telle interprétation conduirait impliquerait notamment[44] de soumettre le traitement de ces données aux conditions générales de cette plateforme, ce qui ne serait pas acceptable.

35. Par ailleurs, à défaut d'encadrer très clairement les conditions de cette communication, les préposés du responsable du traitement (travaillant par exemple dans un dispatching), sont susceptibles de prendre connaissance de données traumatisantes, que les limites de leurs missions ou leurs compétences techniques ne leur permettra peut-être pas de traiter « utilement » voire de manière licite.

36. Enfin, si la disposition est maintenue, il appartiendra au législateur de prendre position sur la délicate question de l'identification de la personne à l'origine de la communication des images et du son. Une telle identification ne pourra bien entendu intervenir que si elle s'avère nécessaire et proportionnée au regard des finalités qui seront déterminées dans le projet (au même titre que les autres éléments essentiels du traitement). En d'autres termes, il conviendra de prendre en compte le risque de non déclaration d'incidents par crainte, dans le chef du « *spectateur* » concerné, d'avoir à justifier de sa présence sur les lieux de l'incident.

37. A défaut de prendre en compte l'ensemble de ces éléments, l'Autorité estime que l'art. 10, §4 du projet doit s'abstenir de mentionner la possibilité de communication d'images et de sons par des particuliers.

[43] Une plateforme over-the-top, c'est-à-dire proposant des services de communication convoyés sans recourir à un opérateur téléphonique

[44] Outre la question des transferts internationaux de données

4. Délai de conservation

38. 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.

39. L'art. 9 du projet prévoit une durée de conservation maximale d'un mois à compter de l'enregistrement. Cependant, cette durée est portée à 12 mois pour les images et les sons utiles à l'examen et à l'évaluation d'interventions. Il est en outre prévu les images et les sons qui contribuent à apporter une preuve dans le cadre d'une procédure en justice sont conservés durant le délai requis par cette procédure.

40. L'Autorité rappelle qu'en matière de vidéosurveillance, la conservation des images sous une forme permettant l'identification d'une personne concernée doit également être garantie durant une période minimale durant laquelle l'accès de la personne concernée à ses données doit être garanti. Il y a donc lieu de prévoir ce délai minimal et d'assortir sa méconnaissance d'une sanction.

41. L'Autorité estime par ailleurs que la conservation des données utiles à l'examen et à l'évaluation d'interventions au-delà du 1er mois, n'est pas suffisamment justifiée, en termes de nécessité et de proportionnalité[45], dans le commentaire de l'art. 9. Un libellé satisfaisant à cet égard devra comporter des critères objectifs permettant au responsable du traitement d'évaluer le caractère utile de la conservation d'images et de son, comportant des données à caractère personnel. Si ce caractère nécessaire et proportionné devait pouvoir être démontré, il y aurait néanmoins lieu d'informer les personnes concernées du traitement de leurs données à caractère personnel à des fins de sensibilisation ou d'information et de leur permettre de s'opposer à ce traitement.

42. Enfin, les données à caractère personnel traitées à des fins probatoires dans le cadre d'une procédure judiciaire doivent être communiquées à un autre responsable du traitement dans ce cadre et le délai de conservation applicable est celui prévu par les règles de procédure. L'Autorité estime que cet alinéa est susceptible de laisser croire – à tort - que la conservation, par le responsable du traitement concerné par la procédure, d'une copie de l'enregistrement serait autorisée dans ce cas. Par conséquent, il convient d'omettre le dernier alinéa de l'art. 9.

[45] Par exemple par rapport à une solution visant à faire « rejouer » une intervention particulièrement instructive par des acteurs ; Pour rappel, la Cour de justice estime « *que le manque de ressources allouées aux autorités publiques ne saurait **en aucun cas** constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte* » (CJUE, 1er août 2022, C-184/20, OT c. Vyriausioji tarnybinės etikos komisija**,** §89)

5. Responsable du traitement

43. L'art. 14 du projet désigne des responsables « *opérationnels* » du traitement. Seul le commentaire de l'art. 14 désigne expressément « *le SPF Intérieur pour les unités opérationnelles de la protection civile et des zones de secours elles-mêmes en ce qui les concerne* » en tant que responsable du traitement. Ajoutant que la doctrine considère unanimement qu'il doit s'agir de l'autorité et non du dirigeant.

44. L'Autorité estime qu'il y a lieu de nuancer cette affirmation. En effet, les lignes directrices de l'EDPB précisent au contraire « *qu'il n'existe, en principe, pas de limitation quant au type d'entité susceptible d'assumer le rôle de responsable du traitement. Il peut s'agir d'une organisation, mais également d'un individu ou d'un groupe d'individus*[46]*. Toutefois, dans la pratique, c'est généralement l'organisation en tant que telle, et non une personne au sein de celle-ci (comme le directeur général, un salarié ou un membre du conseil d'administration), qui agit en tant que responsable du traitement au sens du RGPD* »[47].

45. En réalité la désignation des responsables du traitement doit être adéquate au regard des circonstances factuelles[48]. En d'autres termes, il est nécessaire de vérifier pour chaque traitement de données à caractère personnel qui, *dans les faits*, poursuit la finalité pour laquelle elles sont traitées et dispose de la maîtrise des moyens utilisés pour atteindre cette finalité.

46. Or, à la lecture du rôle assigné aux responsables opérationnels du traitement[49] par les art. 14, 15 et 17 du projet (décider de l'objectif du traitement et des moyens utilisés pour y parvenir, s'assurer que les principes de finalité, de proportionnalité, de subsidiarité et d'efficacité sont respectés, réaliser une analyse d'impact relative à la protection des données, tenir un registre des activités de traitement ainsi qu'un registre reprenant toutes les utilisations effectives de caméras au sein du service opérationnel de la sécurité civile concerné, etc…), l'Autorité estime qu'en l'espèce la désignation du SPF et des Zones de secours serait inutilement formelle et doit être abandonnée au profit d'une requalification des responsables opérationnels en responsables du traitement.

---

[46] À titre d'exemple, dans son arrêt dans l'affaire Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:551, point 75, la Cour de justice a jugé qu'une communauté religieuse de témoins de Jéhovah a agi comme un responsable du traitement conjointement avec ses membres individuels.

[47] EDPB, Lignes directrices 07/2020 adoptées le 7 juillet 2021 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 11 (https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_fr.pdf)

[48] En effet, tant le Comité européen à la protection des données que l'Autorité insiste sur la nécessité d'approcher le concept de responsable du traitement dans une perspective factuelle. Voir : Comité européen à la protection des données, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted on 02 september 2020, p 10 et s (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en) et Autorité de protection des données, *Le point sur les notions de responsable de traitement/sous-traitant au regard du au regard du Règlement EU 2016/679 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats*, p.1..(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Notions_RT_ST.pdf).

[49] A savoir, « *le commandant de zone, pour ce qui concerne la zone de secours, et le Président du Comité de direction du Service public fédéral Intérieur pour ce qui concerne les unités opérationnelles de la protection civile* »

6. Accès/destinataires

47. En ce qui concerne la visionnage des images prévu l'art. 10 du projet, l'Autorité estime que le libellé actuel pourrait être acceptable pour autant que les caméras de surveillance et de contrôle de lieux, placées et utilisées à des fins de prévention ou de constatation des infractions contre les personnes ou les biens continue à relever de la loi caméras. Cependant même dans ce cas, il serait opportun[50] de distinguer plus finement les possibilités de visionnage en temps réel et pendant l'incident par d'autres responsables du traitement (même sous la supervision du personnel des services opérationnels de la sécurité civile).

48. L'Autorité estime que (sauf à en démontrer le caractère nécessaire et proportionné dans le commentaire de l'art. 10), il y a lieu de limiter un visionnage en temps réel[51], par des tiers, aux finalités liées à la planification d'urgence et de la gestion de situations d'urgence, telles que réglées par l'arrêté royal relatif à la planification d'urgence.

49. En ce qui concerne les personnes qui assurent la permanence d'un dispatching mixte, plutôt que de prévoir leur accès en temps réel ou pendant l'événement, sans davantage d'explications, il convient de déterminer en quoi cette situation devrait différer de l'accès des services de police, prévu par la loi caméra et, le cas échéant, s'ils s'agit de données policières (au sens du Titre II LTD) traitées par les personnes n'appartenant pas aux services de police en qualité de sous-traitant ou s'il s'agit de mettre en œuvre des règles de gestion de l'information distinctes.

50. En ce qui concerne les personnes invitées, il convient de déterminer objectivement et avec davantage de précision quelles personnes sont susceptibles d'être invitées ou non. Une disposition correctement libellée à cet égard devra notamment permettre de déterminer si une autorité administrative d'une zone non concernée par un incident serait susceptible d'être invitée dans un poste de commandement opérationnel et, ce faisant, d'avoir accès aux images. Dans l'affirmative, il appartient bien entendu au législateur de démontrer le caractère nécessaire et proportionné d'une telle mesure et de commenter la disposition de manière à permettre aux responsables du traitement d'identifier si les conditions d'une telle invitation sont réunies.

7. Limitation des droits de la personne concernée

51. L'article 23 du RGPD autorise les États membres à limiter la portée des droits des personnes concernées, à condition toutefois que cette limitation respecte l'essence des libertés et droits

[50] Alors qu'en cas de dérogation à la loi caméras et/ou de recours à des bodycams (cfr. *infra*) ce serait indispensable

[51] C'est-à-dire dans des circonstances ne permettant pas de mettre en œuvre le principe de minimisation des données

fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour atteindre un des objectifs légitimes énoncés par l'article 23.1 du RGPD, comme par exemple, la sécurité nationale, la sécurité publique, ou encore d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale, en particulier une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique.

52. En l'espèce, l'art. 17 du projet permet au responsable opérationnel du traitement de refuser de faire droit à une demande d'accès lorsqu'il existe un danger pour la sécurité publique ou un risque de porter atteinte aux droits et libertés d'autrui ou lorsque les images et/ou les sons concernés par la demande sont utilisés dans le cadre d'une procédure pénale.

53. Le libellé de cette disposition - qui n'est pas davantage explicitée dans le commentaire - ne permet pas de comprendre dans quelles situations l'accès par la personne concernée à ses données propres données, collectées par des services de sécurité civile seraient susceptibles de rencontrer les conditions d'une telle limitation. L'Autorité estime que cette disposition est susceptible de conduire à des refus d'accès illégitimes et qu'à défaut d'être clarifiée et illustrée par des exemples concrets, il convient de l'omettre.

54. A défaut d'omettre cette disposition, l'Autorité rappelle que toute mesure législative prévoyant des limitations aux droits de la personne concernée doit au moins contenir des dispositions spécifiques relatives aux éléments énumérés à l'article 23.2 du RGPD, à savoir :
    - les finalités du traitement ou des catégories de traitement,
    - les catégories de données à caractère personnel,
    - l'étendue des limitations introduites,
    - les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites,
    - la détermination du (des) responsable(s) du traitement (ou des catégories de responsables du traitement),
    - les durées de conservation,
    - les risques pour les droits et libertés des personnes concernées et
    - le droit des personnes concernées d'être informées de la limitation.

55. Afin de déterminer la portée de la marge d'appréciation dont le législateur bénéficie dans ce cadre, il importe de rappeler la jurisprudence de la Cour de justice concernant l'article 13 de la Directive 95/46/CE qui prévoyait également la possibilité de limiter les droits des personnes concernées. Dans l'arrêt *Smaranda Bara*, la Cour a confirmé que ces limitations ne pouvaient être instaurées que par

"*des mesures législatives*"[52]. Ultérieurement, la Cour a précisé que les États membres ne pouvaient adopter ces exceptions que pour autant qu'elles soient "*nécessaires*"[53]. Vu l'intention inchangée du législateur européen d'assurer un niveau élevé de protection des données personnelles[54], les limitations aux droits des personnes concernées doivent être strictement nécessaires pour atteindre l'objectif poursuivi[55]. La nécessité et la proportionnalité de ces limitations doivent donc être interprétées de manière restrictive[56].

8. Cas particulier des bodycams

56. Bien que ni le projet, ni l'exposé des motifs ne fasse expressément référence à l'utilisation de bodycams par les services opérationnels de la sécurité civile[57], l'Autorité précise que **les dispositions actuelles du projet seraient insuffisantes pour permettre l'utilisation de ce type de caméras par les services opérationnels de la sécurité civile**.

57. Une norme permettant le recours à une telle modalité d'utilisation de la technologie, par des services non répressifs, devrait tout d'abord démontrer le caractère légitime de la finalité envisagée. Il faudra ensuite démontrer le caractère nécessaire et proportionné de la mesure, au regard des finalités poursuivies, en fonction des services[58] et des zones de secours concernées[59]. Pour ce faire, il y aura lieu de démontrer, sur base d'éléments factuels et objectifs, l'efficacité du traitement de données à caractère personnel envisagé pour atteindre l'objectif recherché ainsi que le fait qu'il ne soit pas possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel. Il conviendra, à cette fin, de détailler et être en mesure de démontrer, à l'aide d'éléments de preuve factuels et objectifs, les raisons pour lesquelles les autres mesures moins intrusives (telles que le fait de requérir une présence policière[60], qui outre les moyens techniques de collecte de preuves dont elle dispose, a la possibilité

---

[52] Cour de justice, 1er octobre 2015 (C-201/14), *Smaranda Bara e.a.*, § 39 ; Cour de justice, 27 septembre 2017 (C-73/16), *Puškár*, § 96.

[53] Cour de justice, 7 novembre 2013 (C-473/12), *IPI c. Englebert*, § 32.

[54] Considérant 10 du RGPD, considérant 10 de la Directive 95/46/CE.

[55] Ibid., § 39.

[56] Avis n° 34/2018 du 11 avril 2018 *concernant un avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* et plus spécifiquement ses considérants 36 à 38.

[57] Contrairement à la presse (voy. https://www.nieuwsblad.be/cnt/dmf20211001_96876710)

[58] Les chiffres des agressions dont les membres de la protection civile sont victimes permettent-ils de démontrer la nécessité de la mesure ?

[59] A défaut d'être en mesure de démontrer un besoin uniforme, la démonstration de la nécessité de la mesure pourrait être confiée aux autorités locales compétentes à charge pour le projet de ne limiter à prévoir une faculté moyennant le respect de garanties minimales (dont la démonstration du caractère nécessaire et proportionné) par une autorité locale dont la décision est attaquable devant le Conseil d'Etat

[60] Pour rappel, la Cour de justice estime « *que le manque de ressources allouées aux autorités publiques ne saurait **en aucun cas** constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte* » (CJUE, 1er août 2022, C-184/20, OT c. Vyriausioji tarnybinės etikos komisija**,** §89)

de dresser procès-verbal des infractions constatées et surtout d'user de son pouvoir d'exercice légitime de la force publique pour prévenir l'agression des services de secours) ne sont pas suffisantes pour atteindre l'objectif recherché.

58. Si la nécessité du traitement de données à caractère personnel est démontrée, il faut encore démontrer que celui-ci est proportionné (au sens strict) à l'objectif qu'il poursuit, c'est-à-dire qu'il faut démontrer qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement. Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées. Une telle démonstration devrait s'appuyer sur un **rapport objectif**, qu'il convient de soumettre à un débat parlementaire. Ce rapport peut être le résultat d'une phase test, strictement limitée dans le temps par la norme législative qui l'encadre ou un rapport étranger[61].

59. En outre, dans la mesure où le recours à des bodycams ne manquerait pas d'engendrer une atteinte importante aux droits et libertés des personnes concernées, l'Autorité considère que le cadre de l'**analyse d'impact relative à la protection des données** qui est visé à l'article 35 du RGPD constitue une méthodologie adéquate pour examiner la proportionnalité du traitement de données à caractère personnel envisagé par un tel projet. En l'occurrence, l'Autorité estime qu'il est nécessaire que cette analyse d'impact relative à la protection des données soit effectuée à ce stade du processus législatif. On ne peut en effet pas exclure que suite à cette analyse, des prescriptions spécifiques doivent être insérées dans la réglementation.

60. Enfin, une norme encadrant l'utilisation d'un tel moyen technique, même de manière limitée dans le temps dans le cadre d'une phase test, devrait également prévoir :

- que l'utilisation de ces moyens techniques doit être facultative et doit faire l'objet d'une autorisation par une autorité politique compétente pour le périmètre concerné, susceptible de refuser ou de retirer son autorisation en cas d'abus (en d'autres termes, une autorité distincte de celle qui formule la demande[62]) et dont la décision est attaquable devant le Conseil d'Etat[63] ;

[61] Le rapport français n'est à cet égard pas suffisant, puisqu'il démontre tout d'abord une augmentation des faits, suivi d'une chute liée à l'application des mesures de confinement dans le cadre de la pandémie de COVID-19 (https://mobile.interieur.gouv.fr/content/download/133186/1056033/file/20210819%20Rapport%20cam%C3%A9ras.pdf)

[62] Comme le prévoit, de manière malheureuse, l'art. 8 du projet, en particulier en ce qui concerne la protection civile

[63] Pour l'historique de l'implication des Conseils communaux, voy. l'intervention du professeur De Hert dans le rapport de 2006 précité

- l'identité du (des) responsable(s) du traitement (qui, compte-tenu des importantes différences géographiques, ne devrait pas se situer au niveau fédéral) ;
- les règles d'activation et d'utilisation au regard notamment de la nécessité de respecter le secret médical ;
- les (catégories) de données qui sont nécessaires à la réalisation des finalités visées (en ce compris les données d'identification de l'agent porteur de la bodycam et le fait qu'un avertissement ait été donné par cet agent) ;
- le délai de conservation des données (en ce compris le délai endéans lequel la suppression des données relatives à une personne concernée souhaitant accéder à ses données, par exemple dans le cadre d'une procédure, constitue une infraction et la sanction liée à une telle infraction) et la mention de l'obligation de suppression définitive de ces données au terme de ce délai ;
- les (catégories de) personnes concernées dont les données seront traitées (en veillant à déterminer si, par exemple, dans le cadre d'une altercation avec l'agent porteur de la caméra ou avec les services de police, une personne concernée peut demander à ce que la caméra des services de secours soit activée et, dans la négative, quelle pourrait être la justification d'un tel refus) ;
- les destinataires ou catégories de destinataires auxquels les données seront communiquées (en appliquant une échelle de gradation liée à l'ampleur de la situation d'urgence rencontrée) ;
- les circonstances dans lesquelles elles seront communiquées ;
- le cas échéant la limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD (étant entendu que, même en cas d'utilisation à des fins probatoires, les données collectées ne sont pas des données policières et le responsable du traitement ne pourrait donc pas invoquer le secret de l'enquête ou de l'instruction pour limiter l'accès de la personne concernée à ses données) ; ainsi que
- les mesures de sécurité applicables (dont le chiffrement, l'effacement automatique[64] et la journalisation des traitements).

61. L'Autorité précise que la neutralité technologique (qui est une préoccupation légitime) ne peut être valablement invoquée pour s'opposer à une règlementation spécifique et détaillée, des modalités d'utilisation d'une caméra portée par des agents de services non policiers.

[64] Les dispositifs (de type dashcams) qui conditionnent la conservation des données à une manipulation spécifique (et non l'effacement des données, qui est quant à lui, automatique) sont, le cas échéant, à privilégier. Ceci constitue en effet une garantie efficace contre l'oubli d'effacement.

62. Il résulte de ce qui précède que, si la demanderesse souhaite permettre le port de bodycams par les agents de certains services opérationnels de la sécurité civile, le projet devra être fondamentalement revu en tenant compte des observations formulées ci-avant[65]. **Le cas échéant, l'Autorité souhaite que le projet modifié, accompagné de l'analyse d'impact relative à la protection des données lui soit soumis avant la mise en œuvre des traitements**. L'Autorité estime par ailleurs qu'au vu de l'impact sur les droits et libertés des citoyens, un tel projet devrait être soumis à l'Institut fédéral des Droits humains (IFDH) pour avis.

PAR CES MOTIFS,
L'Autorité
estime que :

- il y a lieu d'appliquer la lois caméras aux caméras utilisés par les services de secours pour des finalités liées à la surveillance et le contrôle des lieux aux fins de prévenir, constater ou déceler des infractions contre les personnes ou les biens (points 11 et 18) ;
- il convient de prévoir que des statistiques seront réalisées par chaque responsable du traitement des données collectées par des caméras placées sur l'espace public, aux fins de la publication d'un rapport d'évaluation périodique portant sur l'efficacité de chacune des caméras de surveillance déjà installées, par rapport aux finalités pour lesquelles leur placement a été considéré comme justifié (point 13) ;
- à défaut d'appliquer la loi caméras, le projet doit comporter des règles, être suffisamment précis et donner suffisamment de garanties en ce qui concerne l'utilisation de caméras de surveillance (point 19) ;
- l'art. 7, §3 du projet doit être reformulé de manière à prévoir une interdiction du placement et de l'utilisation des caméras visées par le projet « *d'une manière qui prendre possible le traitement de catégories particulières de données au sens de l'art. 9 du RGPD* » (point 20) ;
- les traitements susceptibles d'être effectués à l'égard de données relatives à une infraction pénale doivent être mentionnés à l'art. 7, §4 du projet (point 21) ;
- à défaut d'une interdiction de placement et d'utilisation de caméras intelligentes reliées à un

[65] Le cas échéant, la demanderesse pourra s'inspirer de la délibération de la CNIL n°2019-056 du 9 mai 2019 concernant un projet de décret relatif aux conditions de l'expérimentation de l'usage de caméras individuelles par les sapeurs-pompiers dans le cadre de leurs interventions, JORF n°0166 du 19.07.2019, pp. 91 et sv.
(https://www.legifrance.gouv.fr/download/pdf?id=e6bxMYSEEHfqF4oOYmAHPcIhrqwujdx3mpjV630EYeg=) ; voy. également (en tenant compte du fait que le contexte policier ne peut être transposé tel quel à une utilisation par des services civils) l'avis d'initiative du COC n°CON190008 du 8 mai 2020 rendu suite aux constatations dans le cadre d'une enquête sur l'utilisation de bodycams (https://www.organedecontrole.be/files/CON19008_Avis_dOffice_COC_Bodycam_F.PDF)

fichier de données à caractère personnel, la transposition des dispositions relatives aux caméras intelligentes « *couplées* », issues loi applicable aux services de police dans l'exercice de leurs missions de police administrative et judiciaire, doit faire l'objet d'une justification en termes de nécessité et de proportionnalité, dans le commentaire de l'art. 5 du projet (point 26) ;

- l'encadrement de l'enregistrement des données, prévu à l'art. 9 du projet, doit être revu (point 26) ;
- les informations relatives à la stratégie d'anonymisation figurant dans le commentaire de l'art. 7 du projet doivent être adaptées (point 27 à 31) ;
- l'art. 7 du projet doit être modifié en vue d'indiquer, en ce qui concerne l'archivage, que « *sans préjudice de la loi du 24 juin 1955 relative aux archives, un traitement ultérieur des images et du son aux fins d'archivage ne peut intervenir qu'après anonymisation des données à caractère personnel* » (point 32) ;
- l'art. 10, §4 du projet doit s'abstenir de mentionner la possibilité de communication d'images et de sons par des spectateurs ou être fondamentalement revu (points 33 à 37) ;
- l'art. 9 du projet doit prévoir délai minimal de conservation et assortir sa méconnaissance d'une sanction (point 40) ;
- le caractère nécessaire et proportionne de la conservation des données utiles à l'examen et à l'évaluation d'interventions au-delà du 1er mois doit être démontrée dans le commentaire de l'art. 9 (point 41) ;
- il convient d'omettre le dernier alinéa de l'art. 9 (point 42) ;
- la désignation du SPF et des Zones de secours doit être abandonnée au profit d'une requalification des responsables opérationnels en responsables du traitement (point 46) ;
- il y a lieu de limiter un visionnage en temps réel, par des tiers, aux finalités liées à la planification d'urgence et de la gestion de situations d'urgence, telles que réglées par l'arrêté royal relatif à la planification d'urgence (point 48) ;
- les règles de gestion de l'information applicables aux personnes qui assurent la permanence d'un dispatching mixte doivent être clarifiées (point 49) ;
- il convient de déterminer objectivement et avec davantage de précision quelles personnes sont susceptibles d'être invitées ou non (point 50) ;
- la limitation des droit d'accès prévue à l'art. 17 du projet doit être, soit omise, soit clarifiée, illustrée par des exemples concrets et assortie de garanties (points 53 et 54) ;
- les dispositions actuelles du projet sont insuffisantes pour permettre l'utilisation de bodycams par les services opérationnels de la sécurité civile (points 56 à 62) ;
- si la possibilité d'usage de bodycams devait être prévue (ou maintenue), même dans le cadre d'une phase test, le projet modifié, accompagné de l'analyse d'impact relative à la protection des donnée, doit être resoumis à l'Autorité avant la mise en œuvre des traitements (point 62) ;

- le cas échéant, un tel projet devrait être soumis à l'Institut fédéral des Droits humains (IFDH) pour avis (point 62).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière - Directrice