



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n°222/2026 du 15 octobre 2026

Objet : Avis concernant un projet de loi modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, la loi du 15 mai 2007 relative à la création du service des gardiens de la paix et à la modification de l'article 119bis de la nouvelle loi communale, et la loi du 15 mai 2007 relative à la sécurité civile afin de permettre l'utilisation des caméras individuelles (ADV-2026-00146)

Mots-clés : Bodycams – Caméras individuelles – Personnel non-policier – Phase test – Autorisations susceptibles de recours – Avertissement – Limitation des droits des personnes concernées - Cybersécurité

Version originale

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

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

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

Vu la demande d'avis de Monsieur Bernard Quintin, Ministre de la Sécurité et de l'Intérieur, chargé de Beliris (ci-après « le demandeur »), reçue le 4 septembre 2026 ;

Vu les informations complémentaires sollicitées le 17 septembre 2026 et reçues le 23 septembre 2026 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 15 octobre 2026, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demandeur a sollicité l'avis de l'Autorité concernant un projet de loi modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, la loi du 15 mai 2007 relative à la création du service des gardiens de la paix et à la modification de l'article 119bis de la nouvelle loi communale, et la loi du 15 mai 2007 relative à la sécurité civile afin de permettre l'utilisation des caméras individuelles (ci-après « le Projet »).
2. Le Projet entend mettre en œuvre l'accord de gouvernement, lequel prévoit d'élargir « *encore les possibilités légales concernant l'utilisation de caméras* » et de veiller « *à ce que, nos services de secours, les services publics de transports en commun (De Lijn, TEC et STIB) et les conducteurs de train sur les lignes les plus sujettes aux incidents puissent également après une formation adéquate et dans un cadre bien défini qui respecte la législation en matière de vie privée, recourir aux «bodycams» ou aux caméras de surveillance* »¹.
3. Suite à la survenance d'incidents faisant 5 blessés parmi les membres du personnel de De Lijn à l'occasion d'un contrôle à De Haan, fin mai 2026, le Gouvernement fédéral a annoncé que le Conseil des Ministres avait adopté² un avant-projet de loi réglementant l'utilisation de bodycams (visées par la notion « caméras individuelles » dans le Projet et dans le reste du présent avis) pour les « *services susceptibles d'être confrontés à des actes de violence à l'occasion de l'exercice de leurs fonctions* »³.
4. Le Projet va toutefois plus loin qu'annoncé dans l'accord de gouvernement, puisque son art. 5 vise :
 - les services opérationnels de la sécurité civile ;
 - les conducteurs et agents des services de transport public ;
 - les agents assermentés chargés du contrôle et de la constatation d'infractions ;
 - le personnel d'accompagnement des trains ;
 - les agents de gardiennage pour les activités de gardiennage d'événements et de réalisation de constatations ; et
 - les gardiens de la paix-constatateurs.
5. De plus, le Roi peut, par arrêté délibéré en Conseil des ministres, étendre ce champ à d'autres catégories de membres du personnel relevant d'une autorité publique ou intervenant dans le cadre d'un service organisé par ou pour une autorité publique. La note au Conseil des Ministres accompagnant le

¹ https://www.belgium.be/sites/default/files/resources/publication/files/Accord_gouvernemental-Bart_De_Wever_fr.pdf, p. 140

² Le 22 mai 2026 (<https://news.belgium.be/fr/utilisation-de-bodycams-par-des-categories-de-personnel-non-policier>)

³ <https://www.vrt.be/vrtnws/nl/2026/05/26/regering-maakt-bodycams-mogelijk-voor-personeel-van-openbaar-ver/>

Projet évoque par ailleurs le fait d'étudier l'extension des possibilités de port de caméras individuelles par des agents de gardiennage⁴ à l'accueil des hôpitaux, dans les aéroports et dans les domaines récréatifs.

6. A noter qu'en ce qui concerne les services opérationnels de la sécurité civile, le Projet succède à un précédent projet⁵ devenu la loi du 21 février 2024 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, au sujet duquel l'Autorité a rendu l'avis n° [114/2023](#). **L'Autorité renvoie aux §§57 et sv.⁶ de cet avis pour tout ce qui n'est pas explicitement indiqué dans le présent avis.**

⁴ Dans le cadre de l'activité visée à l'art. 3.13° de la loi relative à la sécurité privée.

⁵ Doc. Parl. Ch., 16 janvier 2024, 55-3769/001, 2023-2024.

⁶ L'Autorité avait indiqué qu'une norme permettant le recours à des caméras individuelles, 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 et des zones de secours concernées. 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 policière⁶, qui outre les moyens techniques de collecte de preuves dont elle dispose, a la possibilité 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.

*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. 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.*

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) et dont la décision est attaquantable devant le Conseil d'Etat ;*
- *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*

I.1. Modification de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance (ci-après « loi caméras »)

7. Les **finalités** d'« utilisation »⁷ des **caméras individuelles** prévues par le Projet sont :
 - la protection de la sécurité des agents ;
 - la dissuasion des comportements agressifs, la désescalade des situations conflictuelles ; et
 - la constatation objective d'incidents⁸ susceptibles de mettre en danger des personnes ou des biens dans un contexte de violence contre les personnes (art. 6)⁹.
8. L'art. 6 du Projet dispose également que les caméras individuelles sont équipées d'une fonction de pré-enregistrement de 30 secondes et l'activation doit être précédée d'un **avertissement oral** « *dès que les circonstances le permettent* ». Il peut par ailleurs être dérogé à l'obligation d'avertissement¹⁰.
9. L'art. 8 impose la tenue, par chaque responsable du traitement compétent, d'un **registre des activations** de caméras individuelles pour chaque catégorie de porteurs. Sont consignées dans ce registre « *automatiquement ou immédiatement après leur enregistrement* » :
 - 1° les enregistrements audiovisuels ;
 - 2° le moment et la période de l'utilisation ;
 - 3° l'identification du porteur de la caméra individuelle qui en a fait usage ; et
 - 4° le lieu ou le trajet pour lequel les données ont été conservées.
10. Ces données sont conservées au minimum pendant 30 jours et au maximum pendant 90 jours.
11. Les **finalités** du traitement des données enregistrées dans le **registre** sont :

-
- les mesures de sécurité applicables (dont le chiffrement, l'effacement automatique et la journalisation des traitements).

⁷ Le commentaire de l'art. 6 utilise le terme « activation ».

⁸ Le commentaire de l'art. 6 précise que la notion « d'incident » vise « toute situation concrète présentant un risque pour la sécurité des personnes ou des biens, ou susceptible de générer une tension ou une contestation dans le cadre de l'intervention, à l'exclusion des interactions ordinaires » et que « le simple fait de constater une infraction, en ce compris en matière de stationnement ou de contrôle de titres de transport, ne constitue pas en soi un incident ». Sont en revanche susceptibles de constituer des incidents justifiant l'activation d'une caméra individuelle « des comportements susceptibles de porter atteinte à des biens ou de provoquer des dégradations ».

⁹ L'art. 7 ajoute que « les caméras individuelles **ne peuvent être utilisées dans le but de** capter ou de traiter des informations relatives à l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance syndicale, son état de santé, sa vie sexuelle ou son orientation sexuelle ».

¹⁰ Lorsque l'activation:

1° peut mettre en danger la sécurité du porteur de la caméra individuelle ou des personnes présentes ;

2° ou est matériellement impraticable vu le nombre de personnes présentes à prévenir ou étant donné que les personnes à avertir sont en danger immédiat ou en état de conscience altérée ;

3° ou est manifestement inappropriée ou inutile, en particulier lorsque la caméra individuelle est utilisée à un endroit dépourvu de présence humaine.

1° rédiger un rapport relatif à des faits survenus dans l'exercice d'une mission légale ou réglementaire, en vue de sa transmission aux services internes ou à l'autorité compétente pour traiter ces faits sur le plan administratif ou judiciaire en vue d'imposer des sanctions administratives ou judiciaires ;
2° apporter un soutien lors de la formation ou de l'accompagnement professionnel ou pour améliorer les processus de sécurité¹¹ ;
3° traiter les plaintes liées à une intervention, un comportement ou un incident impliquant un porteur de caméra ou un tiers.

12. Avant extraction, aucun service externe ne dispose d'un accès direct aux données contenues dans le registre. Après extraction et transmission de ces données aux destinataires énumérés à l'art. 8¹², pour les finalités susmentionnées, ces données sont conservées selon les règles propres à chacune des procédures susmentionnées. Les modalités de transfert de données de la caméra vers le serveur ne sont cependant pas encadrées.
13. Les consultations et les extractions de données ou des enregistrements sont **journalisées**. Les journaux sont conservés pendant 3 ans.

I.2. Modification de la loi du 2 octobre 2017 réglementant la sécurité privée et particulière

14. L'art. 10 du Projet modifie la loi du 2 octobre 2017 réglementant la sécurité privée et particulière en vue de permettre aux **agents de gardiennage** d'utiliser des caméras individuelles pour les activités de gardiennage d'événements et de réalisation de constatations.
15. La même disposition conditionne l'utilisation de caméras individuelles dans le cadre de l'exercice d'activités de gardiennage à l'information et l'**autorisation formelle et expresse** du mandant ou du gestionnaire du lieu « *surveillé* ».
16. Cette disposition prévoit également que le responsable du traitement des données enregistrées dans le registre des activations des caméras individuelles est une personne qui assure la direction effective de l'entreprise de gardiennage ou du service interne de gardiennage.

¹¹ A condition que les données soient anonymisées sauf si cela compromet la finalité poursuivie, dans lequel cas, elles sont pseudonymisées.

¹² *1° les membres des services de police qui ont le besoin d'en avoir connaissance pour l'exercice de leurs missions légales prévues aux articles 14 et 15 de la loi sur la fonction de police ;*

2° les autorités administratives et services internes compétentes pour l'imposition de sanctions administratives ainsi que les autorités judiciaires agissant dans le cadre de l'exercice de leurs missions légales;

3° les autorités, les services et les personnes désignées par le responsable du traitement compétentes pour le traitement des plaintes ;

4° les membres, chargés de la formation ou de l'accompagnement professionnel ou de l'amélioration des processus de sécurité et désignés par le responsable du traitement.

17. L'art. 11 modifie la même loi en vue de permettre aux **agents de sécurité des sociétés publiques de transports en commun** d'utiliser des caméras individuelles.

I.3. Modification de la loi du 15 mai 2007 relative à la création de la fonction de gardien de la paix, à la création du service des gardiens de la paix et à la modification de l'article 119bis de la nouvelle loi communale

18. L'art. 12 du Projet modifie la loi du 15 mai 2007 relative à la création de la fonction de gardien de la paix, à la création du service des gardiens de la paix et à la modification de l'article 119bis de la nouvelle loi communale en vue de permettre aux **gardiens de la paix-constatateurs** d'être équipés¹³ de caméras individuelles et désigne la commune (représentée par le collège communal) ou, le cas échéant, la personne morale de droit public dont dépend le service des gardiens, comme responsable du traitement.

I.4. Modification de la loi du 15 mai 2007 relative à la sécurité civile

19. Les articles 13 à 29 modifient la loi du 15 mai 2007 relative à la sécurité civile en vue de permettre à un membre du personnel d'un service opérationnel de la sécurité civile qui porte et active une **caméra individuelle d'assistance en temps réel à l'intervention** dans l'objectif initial d'aide à l'intervention¹⁴, et qui se trouve confronté à une situation d'agression ou de risque d'agression, d'utiliser cette caméra également dans un objectif de protection. En vertu du Projet une telle utilisation reste intégralement soumise aux dispositions de la loi du 15 mai 2007 relative à la sécurité civile et non à la loi caméras.
20. A la différence de la caméra individuelle (classique), la caméra individuelle d'assistance en temps réel à l'intervention réalise des enregistrements audiovisuels et permet la transmission en temps réel ou pendant un incident, d'images, de sons et de données GPS ainsi que la réception de communications audio (sans avoir à faire usage de la radio)¹⁵.

¹³ Comme le permet le chapitre IV/1 nouveau de la loi caméras.

¹⁴ Conformément à la modification de la loi du 15 mai 2007 par la loi du 21 février 2024.

¹⁵ Art. 15 du Projet. L'art. 17 modifie les finalités d'utilisation de ces caméras (à savoir *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; 3° repérer des objets, des corps ou des incidents; 4° protéger le personnel et 5° prendre des images et/ou du son dans le cadre de la planification d'urgence et de la gestion de situations d'urgence (...)*), en vue d'y ajouter la finalité de dépôt de plainte et de prévoir que le traitement ultérieur des données GPS n'est autorisé que pour évaluer une intervention.

L'art. 18 du Projet impose que la **demande d'utilisation** de caméras par les services opérationnels de la sécurité civile, adressée par le commandant de zone ou le Président du Comité de direction du Service public fédéral Intérieur au ministre de l'Intérieur ou à son délégué, propose le type de caméras à utiliser ainsi que les modalités d'utilisation (*Les modalités d'utilisation déterminent notamment quand le port de la caméra individuelle d'assistance en temps réel à l'intervention est obligatoire et si l'enregistrement du son est nécessaire ou pas, quand celui-ci peut techniquement être dissocié des images*).

L'art. 19 du Projet fixe la **durée maximale de conservation** des images, des sons ainsi que des données GPS à 30 jours à compter de leur enregistrement, sauf si ces enregistrements sont « *utiles à l'examen et à l'évaluation d'interventions* », auquel

II. EXAMEN DU PROJET

II.1. Remarque liminaire

21. Le formulaire accompagnant la demande d'avis justifie l'application d'un délai abrégé de 30 jours par le fait « *qu'il s'agit d'améliorer rapidement la sécurité et le sentiment de sécurité des groupes professionnels visés, un avis de 30 jours est demandé* » et que « *après l'entrée en vigueur du projet, les groupes professionnels devront encore réaliser une évaluation opérationnelle et d'impact sur la protection des données* ».
22. L'Autorité souhaite rappeler que tous les projets qui lui sont soumis comportent une dimension d'intérêt public plus ou moins importante et qu'elle ne dispose pas des ressources suffisantes pour traiter toutes les demandes qui lui sont soumises en 30 jours. L'Autorité regrette par ailleurs qu'alors que la décision de lui imposer ce délai figurait déjà dans la note au Conseil des Ministres, datée du 22 mai 2026, le Projet ne lui a été soumis que le 4 septembre 2026.

cas ils peuvent être conservés 90 jours, s'ils proviennent de caméras individuelles d'assistance et 365 jours s'ils proviennent d'autres caméras. Au terme de ce délai, la disposition en projet prévoit l'anonymisation des enregistrements conservés à des fins de formation, de sensibilisation ou d'information et la suppression dans les autres cas.

L'art. 20 du Projet permet le **partage** de données en temps réel ou pendant l'incident avec les services de police.

L'art. 24 du Projet¹⁵ ajoute le **trajet** de la caméra et l'identité du porteur à l'énumération des données devant être contenues dans le registre. (L'Autorité relève qu'à partir de l'art. 23, la numérotation du commentaire des articles est en décalage par rapport au texte du Projet)

L'art. 25 du Projet intègre les mêmes exceptions que celles prévues pour les caméras individuelles à l'obligation d'avertissement oral lors de « l'utilisation » d'une caméra. À savoir, lorsque l'avertissement:

1° peut mettre en danger la sécurité du membre du personnel ou des personnes présentes ;

2° est matériellement impraticable vu le nombre de personnes présentes à prévenir ou étant donné que les personnes à avertir sont en danger immédiat ou en état de conscience altérée ;

3° est manifestement inapproprié ou inutile, en particulier lorsque la caméra est utilisée à un endroit dépourvu de présence humaine.

Aux termes de l'art. 28 du Projet, les **finalités** d'utilisation des caméras individuelles d'assistance en temps réel à l'intervention par les services opérationnels de la sécurité civile sont :

1° guider le personnel afin d'assurer la sécurité des membres du personnel opérationnel de la sécurité civile en intervention et la sécurité de tiers présents dans la zone d'intervention ;

2° aider à obtenir un aperçu de la zone d'intervention, et aider à évaluer la situation afin d'intervenir adéquatement ;

3° localiser, via les coordonnées GPS de la caméra individuelle, les membres du personnel opérationnel de la sécurité civile en intervention en cas de nécessité.

Cependant, en cours d'utilisation d'une telle caméra pour l'une des finalités précitées, les **finalités d'utilisation suivantes sont également admises**, à condition que des « *faits susceptibles de constituer une atteinte à l'intégrité physique des membres du personnel, ou de causer des dommages aux biens, ou si la situation présente un risque sérieux d'escalade vers de telles atteintes* » soient survenus :

1° protéger la sécurité des membres du personnel ;

2° favoriser la désescalade des situations conflictuelles ;

3° constater de manière objective le déroulement d'incidents ou de situations mettant en danger la sécurité du membre du personnel, ou causant des dommages aux biens du service opérationnel de la sécurité civile, notamment en cas de violence, afin que ceux-ci puissent être signalés aux services compétents.

23. Ceci étant, l'Autorité entend mettre tout en œuvre pour rendre son avis dans les meilleurs délais, mais demande – dans un souci d'effectivité de l'exercice de ses missions - qu'à défaut pour le législateur de permettre l'extension du cadre de son personnel, il soit veillé à lui permettre de rendre ses avis dans un délai de 60 jours.

II.2. Choix du cadre juridique

24. L'exposé des motifs du Projet indique que le choix d'intégrer l'utilisation des caméras individuelles dans la loi caméras « *s'inscrit dans la continuité des positions exprimées par l'Autorité de protection des données, notamment dans son avis n° [114/2023](#), dans lequel celle-ci a rappelé que, lorsque des caméras sont utilisées par des services de secours ou des services assimilés à des fins de prévention, de constatation ou de déclaration d'infractions contre les personnes ou les biens, elles relèvent du champ d'application de la loi du 21 mars 2007 et doivent être encadrées par celle-ci* ».

25. **Sans remettre en cause le principe de l'intégration du cadre législatif relatif à l'utilisation des caméras individuelles dans la loi caméras**, l'Autorité tient à préciser que les §§11 à 18 de son avis précité visaient les dispositions d'un projet visant à exclure les caméras des services opérationnels de la sécurité civile¹⁶ 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* »¹⁷. En d'autres termes, l'Autorité voulait expliquer au demandeur ¹⁸ que si les zones de secours souhaitent installer des caméras de surveillance pour sécuriser leurs locaux, rien ne justifiait de ne pas faire relever ces caméras de la loi caméras. Il s'agit donc d'un cas de figure distinct du déploiement des caméras individuelles.

II.3. Importance de l'ingérence

26. L'Autorité constate que **l'ingérence** résultant des traitements de données prévus par le Projet revêt un **caractère particulièrement important**, en raison de la possibilité pour les caméras individuelles de capter, à très faible distance, des personnes concernées (et dans toute une série de lieux accessibles au public, y compris des lieux sensibles et même devant ou, plus exceptionnellement, dans le domicile

¹⁶ 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

¹⁷ L'exposé des motifs du projet précisait par ailleurs 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* », sans toutefois que les difficultés rencontrées dans la pratique ne soient mentionnées dans ledit exposé des motifs.

¹⁸ Par « *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...* » (§11).

de la personne concernée), à la fois des images et du son (et donc d'enregistrer des visages et des voix)¹⁹.

27. Bien que les dispositions en projet ainsi que leurs commentaires aient été rédigés avec un sérieux en ligne avec l'importance de l'ingérence, l'Autorité identifie ci-après les **modifications indispensables** pour atteindre le niveau de prévisibilité requis par le principe de légalité et pour assurer le caractère nécessaire et proportionné des traitements de données qu'impliquent l'utilisation, par les services concernés, de caméras individuelles.

II.4. Finalités des traitements de données à caractère personnel envisagés

1) Loi caméras

1.1. Finalités d'utilisation des caméras

28. Tout d'abord, l'Autorité estime que, dans la perspective d'encadrer un traitement de données à caractère personnel, le terme « *utilisation* » manque de précision (contrairement au terme « activation », mentionné dans le commentaire de l'art. 6 du Projet). Cependant, l'Autorité comprend que la protection des données ne soit pas la seule préoccupation des auteurs du Projet et que l'utilisation de telles caméras mérite d'être encadrée également. L'Autorité recommande donc de **distinguer les raisons pour lesquelles le « port » d'une caméra individuelle, par un service, peut être autorisé et de prévoir ensuite les finalités d'« activation » de la caméra par un membre de ce service**²⁰.
29. Ensuite, l'Autorité estime que la finalité relative à la protection de la **sécurité** « *des agents* » devrait être précisée, pour ne viser que « *l'agent porteur* ».
30. Interrogé au sujet de la finalité de « **constatation objective d'incidents** », le fonctionnaire délégué a indiqué que le risque d'engendrer une escalade par le fait d'activer une caméra individuelle pour une

¹⁹ 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* » (Lignes directrices [03/2019](#) adoptées le 29 janvier 2020, point 1).

²⁰ En effet, le fait de porter de manière ostensible une caméra individuelle peut déjà suffire à atteindre les objectifs de protection de la sécurité des agents, la dissuasion des comportements agressifs et la désescalade des situations conflictuelles. Cependant, le seul port d'une telle caméra n'implique pas un traitement de données à caractère personnel, mais doit néanmoins être encadré, puisque ce port rend une activation et donc une ingérence dans les droits et libertés des personnes concernées, possible. À l'inverse, la finalité de constatation objective d'incidents ne peut se concevoir que concomitamment à l'activation de ces caméras.

finalité de constatation, ne pouvait pas être exclu²¹. Il ajoute que c'est la raison pour laquelle le Projet « prévoit une formation préalable des porteurs et encadre l'avertissement précédant l'activation, en tenant notamment compte de l'état de vulnérabilité de la personne concernée et des circonstances concrètes de l'intervention ». L'Autorité en prend acte, mais estime qu'il convient d'**établir une hiérarchie des finalités** en prévoyant expressément que « l'activation de la caméra individuelle à des fins de constatation d'incidents ne peut en aucun cas intervenir lorsque le porteur n'est pas directement et personnellement visé par des comportements agressifs et que l'activation est susceptible d'entraîner une escalade et/ou de le mettre en danger »²².

31. Le **caractère « objectif » des constatations** pose par ailleurs question. Interrogé quant à la pertinence de l'utilisation de ce terme, le fonctionnaire délégué a indiqué que la notion d'« *objectivation* » signifie qu'« *il s'agit de disposer d'un enregistrement continu et non modifiable par l'agent concerné, permettant de documenter aussi complètement que possible le déroulement factuel de l'intervention* »²³.
32. L'Autorité estime que la signification attachée par les auteurs du Projet au terme « *objectif* » est admissible. Cependant, afin que le terme « *objectif* » ne puisse pas être interprété comme accordant une valeur probante supérieure à un enregistrement réalisé par une caméra individuelle, par rapport à un enregistrement, non traité, manipulé ou édité²⁴, réalisé par un tiers, alors que dans cette hypothèse, seul l'angle de l'enregistrement serait différent, l'Autorité estime qu'il convient d'**indiquer dans le Projet que pour la finalité de constatation d'incidents, le terme « objective » signifie que les enregistrements réalisés par la caméra individuelle visent autant à protéger les personnes filmées contre d'éventuels comportements abusifs des porteurs qu'à protéger les porteurs contre le dépôt de plaintes infondées**. L'Autorité estime par ailleurs que le commentaire

²¹ Le fonctionnaire délégué se réfère à cet égard au rapport annuel du Comité permanent P qui « relève que la manière dont l'activation d'une bodycam est annoncée peut contribuer à une désescalade ou, au contraire, à une escalade de la violence et souligne, précisément pour cette raison, l'importance d'une formation adaptée, notamment en matière de communication » (Comité permanent P, Rapport annuel 2021, p. 69).

²² En d'autres termes, l'Autorité estime que la facilitation de la répression de dommages causés à des biens ne peut en aucun cas justifier un traitement de données à caractère personnel susceptible de mettre un intervenant en danger.

²³ Le fonctionnaire délégué cite l'exemple du rapport annuel 2023 du Comité permanent P qui « relève que, parmi les 16 plaintes clôturées en 2023 dans lesquelles il était fait référence à une bodycam, l'analyse des images a permis, dans neuf cas, de conclure à l'absence de manquement dans le chef des policiers concernés. Le Comité P constate en outre que les images ont permis de faire la lumière sur le déroulement des interventions et que, dans les cas concernés, l'absence d'images n'aurait pas permis de statuer sur l'existence ou non d'un manquement ». Le fonctionnaire délégué ajoute que « l'expérience montre que les séquences diffusées sur les réseaux sociaux ne présentent généralement qu'une partie d'une interaction ou d'un incident. Elles résultent en outre d'une sélection d'images qui peut avoir pour effet de soutenir un récit particulier plutôt que de restituer l'ensemble du déroulement des faits ». A l'inverse, l'enregistrement réalisé au moyen d'une bodycam « ne peut être traité, manipulé ou édité par l'agent qui procède à l'enregistrement. Il permet de documenter, de manière continue, l'interaction et le déroulement de l'incident, du début à la fin ».

²⁴ Comme il sera indiqué *infra* (au sujet des catégories particulières de données et de l'exercice des droits des personnes concernées), la possibilité d'édition de l'enregistrement par le responsable du traitement voir par le logiciel de la caméra (mais non par le porteur) est cependant une garantie essentielle permettant la mise en œuvre effective du principe de minimisation des données. Cette possibilité d'édition doit donc être expressément prévue dans le Projet.

de l'article concerné devrait rendre compte du fait que plusieurs études ont mis en évidence des **biais** susceptibles de conduire à interpréter erronément un comportement comme étant agressif²⁵.

33. L'art. 7 du Projet ajoute que les caméras individuelles **ne peuvent pas être utilisées** :

- pour l'authentification ou l'identification biométrique, la reconnaissance automatique des émotions ou la catégorisation biométrique ; ni
- **dans le but de** capter ou de traiter des informations relatives à l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance syndicale, son état de santé, sa vie sexuelle ou son orientation sexuelle.

34. L'Autorité accueille favorablement ces interdictions. Toutefois, l'Autorité estime que **la référence au seul objectif (« dans le but de ») est à proscrire**. En revanche, il pourrait être admis de prévoir une interdiction d'activation de l'enregistrement vidéo et/ou audio des caméras visées par le Projet « *dans des circonstances rendant la collecte d'images et de sons comportant des catégories particulières de données au sens de l'art. 9 du RGPD possible, sans être en mesure de démontrer le caractère nécessaire de cette activation* »²⁶. Un tel libellé présente en effet l'avantage de guider le porteur quant à l'application du principe de minimisation (en dépit du fait qu'il ne peut bien entendu pas être attendu de ce dernier qu'il dispose d'une maîtrise sur les propos qui seront tenus par la personne concernée ou le comportement de cette dernière, durant l'incident) et le responsable du traitement quant à l'interdiction de réutiliser les images (non anonymisées) à d'autres fins que celles qui ont justifié l'activation de la caméra.

35. Bien entendu, même si les caméras individuelles ne sont activées que dans des situations parfaitement appropriées, il sera impossible d'éviter complètement que des catégories particulières de données soient traitées²⁷. En dépit de l'obligation, pesant sur le responsable du traitement, de respecter les principes de minimisation des données²⁸ et de protection des données dès la conception²⁹, l'Autorité estime que **le Projet doit comporter les exigences minimales suivantes** :

²⁵ Voy. par exemple Paul B. Hutchings, Geoffrey Haddock, Look Black in anger: The role of implicit prejudice in the categorization and perceived emotional intensity of racially ambiguous faces, Journal of Experimental Social Psychology, Volume 44, Issue 5, 2008, Pages 1418-1420, ISSN 0022-1031, <https://doi.org/10.1016/j.jesp.2008.05.002> (<https://www.sciencedirect.com/science/article/pii/S0022103108000772>)

²⁶ En ce sens, voy. l'ICO guidance on Body Worn Video (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/body-worn-video-bww/>)

²⁷ Tel sera en particulier le cas pour les services opérationnels de la sécurité civile, qui sont susceptibles d'intervenir sur des urgences médicales ou de pénétrer dans des habitations. Mais les autres porteurs potentiels sont également susceptibles de traiter de telle données, par exemple si la personne filmée porte des vêtements aux couleurs de son organisation syndicale.

²⁸ Art. 5.1.c du RGPD

²⁹ Rappelé, en ce qui concerne la conservation, uniquement à l'art. 13/7 nouveau de la loi relative à la Sécurité civile.

- le logiciel back-end³⁰ devra disposer, par défaut, d'une fonctionnalité d'édition automatique des images et du son³¹ capable de flouter ou masquer de manière effective et efficace des parties des enregistrements afin de protéger les droits et libertés des personnes concernées ;
- (sauf à prévoir une interdiction absolue d'activer une caméra individuelle dans les lieux sensibles³²) l'activation pour filmer des personnes dans des lieux sensibles telles que dans une habitation³³, une école ou dans la cellule patient (à l'arrière) d'un véhicule des services d'aide médicale urgente ne peut intervenir, à l'initiative du porteur, qu'en cas d'absolue nécessité (c'est-à-dire en cas de danger grave et imminent pour sa sécurité ou, pour autant que l'activation d'une caméra puisse avoir un effet positif, celle de tiers) démontrable et il ne pourra jamais être dérogé à l'obligation d'information préalable MAIS, si la personne filmée le sollicite, la caméra devra obligatoirement être activée ;

1.2. Finalités des traitements des données du registre « des activations »³⁴

36. Il ressort de l'art. 8 du Projet que le registre des activations ne doit pas être confondu avec un registre des traitements, ni avec un journal. Il s'agit en effet de la **banque de données appelée à contenir les enregistrements audiovisuels**. Ceci implique que les finalités d'enregistrement et de traitement ultérieur des données du registre ne répondent pas à un souci de protection des porteurs, mais de répression (des comportements des tiers ou des porteurs) et de support pédagogique.
37. L'Autorité considère bien entendu que ces finalités sont légitimes. Cependant, en termes de proportionnalité, elles ne sont **pas susceptibles de justifier une ingérence aussi étendue que les finalités liées à la protection de l'intégrité physique des intervenants**³⁵. Le principe de minimisation des données devra donc être appliqué avec davantage de rigueur (par exemple l'effacement automatique après 30 jours et l'édition de l'enregistrement³⁶). Il en va particulièrement ainsi en ce qui concerne la finalité de soutien à la formation (pour laquelle le traitement de données pseudonymisées

³⁰ Installé sur le serveur où les enregistrements seront traités.

³¹ Il s'agit d'une technologie répandue depuis longtemps (voy. <https://www.ojp.gov/pdffiles1/nij/grants/250381.pdf>) et exigée dans les pays précurseurs en matière de recours aux caméras individuelles (voy. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/body-worn-video-bwv/>).

³² Qu'il convient alors de définir dans le Projet.

³³ Ce qui concernera essentiellement les membres des services opérationnels de la sécurité civile.

³⁴ Pour rappel, en vertu de l'art. 8 du Projet, ces finalités sont :

1° rédiger un rapport relatif à des faits survenus dans l'exercice d'une mission légale ou réglementaire, en vue de leur transmission aux services internes ou à l'autorité compétente pour traiter ces faits sur le plan administratif ou judiciaire en vue d'imposer de sanctions administratives ou judiciaires ;

2° apporter un soutien lors de la formation ou de l'accompagnement professionnel ou pour améliorer les processus de sécurité ;

3° traiter les plaintes liées à une intervention, un comportement ou un incident impliquant un porteur de caméra ou un tiers.

³⁵ Sur cette question, voy. *infra*.

³⁶ Ces exemples sont davantage développés *infra*.

ne pourra intervenir que lorsque les enregistrements seront absolument nécessaires pour atteindre cette finalité et que le recours à des données correctement anonymisées³⁷ ne permettra pas d'atteindre l'objectif visé).

38. En outre, cela confirme que, dans certains cas, le simple port ou la « menace » d'activation d'une caméra individuelle peut suffire à atteindre les finalités de protection de la sécurité des agents et de désescalade. La formation dispensée aux porteurs devra tenir compte de cet élément. Compte tenu de ces éléments, l'Autorité considère que **le Projet devrait prévoir que « les porteurs doivent être formés à s'abstenir d'activer leur caméras lorsqu'un avertissement préalable a permis d'atteindre l'objectif de désescalade du conflit ».**

2) Sécurité civile

39. La loi relative à la Sécurité civile vise un type de caméras particulier³⁸ présentant potentiellement un risque accru d'ingérence en raison de la possibilité de transmission d'enregistrements en temps réel³⁹ ainsi que des finalités propres⁴⁰ (tempérant quelque peu ce risque), puisque ce n'est qu'à titre accessoire⁴¹ que ces caméras peuvent également être utilisées dans un objectif de protection du porteur.
40. En ce qui concerne les finalités du traitement des **données GPS**, l'Autorité estime qu'il convient de distinguer plus clairement, dans le Projet, celles qui ne peuvent justifier une communication (ou un accès) en temps réel, de celles qui sont susceptibles de la justifier.
41. L'Autorité ajoute à cet égard qu'il convient de **justifier la raison pour laquelle il est nécessaire que ces données de géolocalisation soient collectées⁴² et surtout transmises** (en temps réel) **via la caméra**. En effet, vu la taille et la manière dont une caméra est portée, le risque de dommage

³⁷ L'Autorité en profite pour attirer l'attention sur l'adoption par l'EDPB des guidelines n° 02/2026, le 7 juillet 2026 (https://www.edpb.europa.eu/system/files/en?file=2026-09/edpb_guidelines_202602_anonymisation_v1_en_0.pdf)

³⁸ Les « caméras individuelles d'assistance en temps réel à l'intervention ».

³⁹ Aux personnes visées à l'art. Art. 13/8. §1er de la loi relative à la sécurité civile, à savoir :

1° les membres du personnel des services opérationnels de la sécurité civile

2° les différentes disciplines, organes de concertation et structures de coordination

3° les personnes qui, dans l'exercice de leurs fonctions, se rassemblent dans une salle de contrôle avec le personnel des services opérationnels de la sécurité civile et ont la nécessité d'en connaître ;

4° les autres personnes, qui, en raison de leurs connaissances ou de leur expertise particulières nécessaires pour l'intervention, sont invitées au sein des organes de concertation ou des structures de coordination.

⁴⁰ 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;

3° repérer des objets, des corps ou des incidents;

⁴¹ Lorsqu'un membre du personnel d'un service opérationnel de la sécurité civile « se trouve confronté à une situation d'agression ou de risque d'agression » (commentaire de l'art. 14 du Projet).

⁴² La collecte pouvant permettre d'associer les métadonnées de localisation à l'enregistrement (et ainsi de vérifier si le membre du personnel était bien là où il prétend être et s'il avait le droit de s'y trouver).

ou de perte de la caméra est bien plus élevé que le risque de perte d'un traqueur GPS intégré dans la tenue d'intervention. Par conséquent, en pareille hypothèse, le traitement des données GPS collectées via une caméra individuelle pourrait ne pas atteindre la finalité de localisation du personnel en intervention. Pire, le traitement de ces données pourrait conduire à mettre en danger le personnel en intervention (par exemple si les secours envoyés pour venir en aide à un collègue en danger sont orientés vers le lieu où la caméra a été désactivée et non vers le lieu où se trouve réellement la personne).

42. Lors de l'adaptation du Projet sur ce point, l'Autorité invite le demandeur à tenir compte du fait que le fait que la technologie intégrant la fonctionnalité GPS à certains modèles de caméras existe, ne constitue pas une justification admissible. Il convient en effet de rédiger les cahiers des charges en fonction de la législation et non en fonction des caractéristiques d'un produit dont on aurait connaissance.
43. Par ailleurs, il convient de prévoir que la communication en temps réel **doit pouvoir être activée et désactivée par le porteur** (tout comme les fonctionnalités d'enregistrement des images et du son par les caméras doivent pouvoir être activées isolément les unes des autres)⁴³.

II.5. Caractère nécessaire et proportionné de la mesure

44. L'exposé des motifs du Projet justifie la nécessité de permettre le port de caméras individuelles par le fait que des agents, « *sans relever des services de police, sont amenés à intervenir dans des contextes sensibles, parfois marqués par des tensions importantes. A titre illustratif, certaines interventions de services de secours, tels que les services d'incendie, peuvent être perturbées par des comportements hostiles visant à la fois les intervenants eux-mêmes et leurs moyens d'intervention, en ce compris les véhicules* ».
45. A la question de savoir si la mesure en projet s'appuyait sur des études scientifiques mettant en évidence une corrélation entre le port de caméras individuelles et la désescalade des tensions, le fonctionnaire délégué a précisé qu'aucune étude spécifique n'avait été lancée dans le cadre de l'élaboration du présent Projet. Le fonctionnaire délégué se réfère toutefois à une étude menée aux Pays-Bas⁴⁴ de laquelle il ressort que « *l'utilisation de caméras individuelles peut avoir un effet désescalant sur les violences commises à l'encontre des fonctionnaires de police* » et ajoute que les caméras individuelles

⁴³ Sans préjudice de la nécessité d'encadrer l'activation (et plus généralement l'utilisation) des caméras individuelles via une procédure contraignante (sur le modèle de ce qui existe au Royaume-Uni : <https://assets.publishing.service.gov.uk/media/5bb769f6ed915d23b3cabd20/safeguarding-body-worn-video-data-01118p.pdf>) afin que la décision d'activation ne puisse pas être prise discrétionnairement par le porteur.

⁴⁴ Evaluatie bodycams Landelijke Eenheid; proeftuin bodycams Dienst Infrastructuur 2018, Sdu Uitgevers, Den Haag; Politie & Wetenschap, Den Haag; Sander Flight, Amsterdam.

ne constituent que l'un des outils d'un ensemble de mesures de prévention, qui combinées entre elles sont susceptibles d'apporter une réponse appropriée aux situations de tension ou d'agression⁴⁵.

46. L'Autorité constate cependant que la méthodologie de l'étude citée ne permet pas de démontrer un véritable lien causal entre le port de bodycams et la diminution de la violence⁴⁶. D'autres études tendent par ailleurs à contester l'existence de pareil lien causal⁴⁷ voire à soupçonner un effet inverse⁴⁸.
47. L'Autorité en conclut que le caractère nécessaire et proportionné de l'extension à des services non policiers de la possibilité de porter des bodycams n'est, à ce stade, pas suffisamment démontré. L'Autorité admet toutefois **que pour apporter cette démonstration, il puisse être nécessaire de passer par une phase test**. A cet égard, l'Autorité accueille favorablement le fait que l'exposé des motifs précise que la mise en œuvre du déploiement des caméras individuelles pourra débuter par des « *projets pilotes (« proofs of concept ») permettant de valider les modalités d'utilisation, d'en mesurer les effets sur le terrain et de garantir que le dispositif répond effectivement aux objectifs poursuivis avant toute extension éventuelle* » et que l'art. 30 du Projet prévoit une évaluation et l'établissement d'un rapport comprenant « *au moins un aperçu quantitatif du déploiement des caméras individuelles dans les différentes catégories de personnel, ainsi qu'une évaluation qualitative de l'utilisation des caméras de surveillance individuelles et un aperçu des difficultés procédurales causées par l'application de cette loi* ».
48. Cependant, en ce que l'évaluation prévue à l'article 30 du Projet ne sera pas indépendante et n'interviendra qu'après 4 ans, elle ne constitue pas un tempérament suffisant permettant d'assurer le caractère proportionné de la mesure.
49. **L'Autorité estime que ce caractère proportionné de la mesure serait garanti si le Projet comportait :**

⁴⁵ « Les auteurs soulignent toutefois que la caméra individuelle ne constitue pas, à elle seule, une réponse aux situations de tension ou d'agression. Elle doit être considérée comme un outil s'inscrivant dans un ensemble plus large de mesures de prévention, de formation et de gestion des situations conflictuelles. C'est la combinaison de ces différents instruments, adaptée aux circonstances concrètes, qui est susceptible d'apporter une réponse appropriée ».

⁴⁶ *De bodycams zijn niet willekeurig verdeeld over een experimentele groep en een controlegroep. Er zijn om die reden ook geen enquêtes gehouden in een controlegroep* (point 3.2, p. 20)

⁴⁷ National Institute of Justice, "Research on Body-Worn Cameras and Law Enforcement," January 7, 2022, [nij.ojp.gov: https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement](https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement)

⁴⁸ Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2016). Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. *European Journal of Criminology*, 13(6), 744-755. <https://doi.org/10.1177/1477370816643734>; Ariel, B., Sutherland, A., Henstock, D. *et al.* Report: increases in police use of force in the presence of body-worn cameras are driven by officer discretion: a protocol-based subgroup analysis of ten randomized experiments. *J Exp Criminol* 12, 453–463 (2016). <https://doi.org/10.1007/s11292-016-9261-3>

- une **disposition abrogatoire** prévoyant l'abrogation de l'ensemble des dispositions en Projet **deux ans** après l'entrée en vigueur de la loi (ce délai pouvant être mis à profit pour évaluer les conclusions d'un rapport indépendant et, le cas échéant, adapter certaines dispositions et, le cas échéant, abroger la disposition abrogatoire) ; et
- une disposition finale **imposant la réalisation d'une étude** (universitaire) **indépendante**⁴⁹, dont les conclusions seraient soumises au ministre compétent pour la Sécurité et l'Intérieur ET à la Chambre des représentants avant toute modification de la disposition abrogatoire ;

50. En outre, en ce qui concerne la détermination des **personnes susceptibles d'être autorisées à porter des caméras individuelles**, le fonctionnaire délégué a précisé qu'outre leur appartenance à l'une des catégories de personnel et l'exercice de l'une des missions citées par le Projet, ces personnes devaient – dans l'exercice de ces dites missions – entrer en contact avec le public ET être exposées de manière objective et récurrente⁵⁰ à des situations de tension, d'agression ou de contestation de leur intervention. Par conséquent, l'évaluation indépendante devra également permettre d'**objectiver** (de manière indépendante et scientifique), en fonction des services concernés, **l'exposition récurrente** à des situations de tension, d'agression ou de contestation de l'action des catégories de porteurs visés par le Projet.

51. Afin de permettre de ne viser que les seuls services pour lesquels un besoin est démontré et surtout de mettre fin à la mesure en cas de disparition du besoin ou lorsque les conditions ne sont pas remplies ou pas respectées, l'Autorité estime que le Projet pourrait **habiliter le Roi à « arrêter [périodiquement], après vérification du besoin opérationnel et du respect des conditions**⁵¹, **la liste des responsables du traitement**⁵² **autorisés à équiper les membres de leur personnel de caméras individuelles** »

 (jusqu'à l'adoption de l'arrêté valable pour la période suivante). L'Autorité estime en effet que l'exigence d'une analyse opérationnelle (par essence très peu transparente) est très insuffisante et est susceptible de permettre d'exonérer les services du Ministre de la Sécurité et de l'Intérieur de toute obligation de contrôle et de toute responsabilité.

⁴⁹ L'Autorité précise que cette exigence ne peut en aucun cas être écartée pour des raisons budgétaires. En effet, la Cour de justice de l'Union européenne 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, 1^{er} août 2022, C-184/20, OT c. Vyriausioji tarnybinės etikos komisija, §89)

⁵⁰ *Le fait qu'ils soient exposés, de manière objective et récurrente, à des situations de tension, d'agression ou de contestation de leur intervention ressort notamment de l'analyse opérationnelle des risques. L'analyse opérationnelle évalue la valeur ajoutée concrète de l'utilisation de caméras individuelles dans l'exercice des missions, en examinant dans quelles situations celles-ci contribuent effectivement à renforcer la sécurité des membres du personnel, à favoriser la désescalade dans les situations conflictuelles ou à objectiver le déroulement des incidents.*

⁵¹ Par le biais l'évaluations et d'audits.

⁵² Comme il sera expliqué *infra* en ce qui concerne les mesures de sécurité (et leur coût), une autorisation visant individuellement les sociétés de gardiennage concernées constitue une garantie essentielle.

II.6. Autorisation

52. L'art. 12/1, §2 *nouveau*, en projet, de la loi caméras prévoit que la décision d'autoriser le port de caméras individuelles appartient au responsable du traitement, sur la base de l'analyse opérationnelle et de l'analyse d'impact relative à la protection des données et dans le respect des mécanismes de concertation applicables.
53. Interrogé à ce sujet, le fonctionnaire délégué précise que cette différence avec le régime des caméras de surveillance fixes dans les lieux ouverts s'explique par la nature du dispositif⁵³.
54. L'Autorité prend acte de l'argument, mais constate tout d'abord qu'un régime d'autorisation est prévu pour les services opérationnels de la sécurité civile. Ensuite, l'Autorité rappelle qu'en raison de la possibilité de capter, à très faible distance, des données vocales et des images relatives à des personnes concernées (dans toute une série de lieux accessibles au public et même devant ou, plus exceptionnellement, dans le domicile de la personne concernée), **les caméras individuelles présentent un risque d'intrusion dans la vie privée des personnes concernées encore bien plus important que des caméras fixes**. De plus, la décision des responsables du traitement **manque de transparence** et **limite** par conséquent **la possibilité d'introduire un recours** contre cette décision.
55. Il en découle, pour l'Autorité, que les observations formulées en 2006 par le professeur De Hert - qui ont abouti à soumettre la décision d'installer des caméras de surveillance à l'avis positif du conseil communal de la commune où se situe le lieu (art. 5, §2 de la loi caméras)⁵⁴ - conservent toute leur pertinence dans le cas d'espèce.
56. Cela étant, l'Autorité comprend que, dans le cas d'espèce, imposer un avis positif des conseils communaux de toutes les communes où ces services peuvent exercer leurs missions, puisse s'avérer être inutilement complexe voire contre-productif en termes de transparence. C'est pourquoi – comme indi-

⁵³ La caméra individuelle n'est pas installée pour surveiller un lieu déterminé : elle constitue un outil lié à l'exercice d'une mission et accompagne son porteur dans l'exercice de celle-ci. Il n'y a dès lors pas lieu de subordonner son utilisation à une autorisation liée au lieu dans lequel la mission est exercée

⁵⁴ A savoir « qu'il serait par contre une bonne idée de laisser aux communes la responsabilité et la possibilité d'intervenir en cas d'abus. Cela ne nécessite pas une très lourde procédure. De cette façon les autorités locales peuvent être associées au contrôle des caméras installés sur leur territoire (...), qu'il proposerait par contre c'est que la dimension publique devienne une responsabilité publique. Quand des communes mènent une politique sécuritaire cela est un droit qui doit être pouvoir réfuté au niveau du Conseil d'Etat.

Le Conseil d'Etat s'est prouvé dans le passé d'être l'instrument idéal pour trouver la juste balance entre le droit à la sécurité et les droits fondamentaux. Il estime donc que l'outil démocratique existe déjà permettant de balancer tous les intérêts en jeu.

L'idéal pour lui serait donc soit d'envisager une réglementation centralisante donnant au SPF de l'Intérieur le pouvoir d'un arbitre, soit de permettre au citoyens un recours auprès du Conseil d'Etat lorsqu'il estiment qu'un système de vidéo-surveillance, installé par un pouvoir public, ne respecte pas leurs droits » (Doc. parl. Sénat, 3-1413/1, 18 avril 2006, 2005-2006, pp. 83-84, <https://www.senate.be/www/?MIval=publications/viewPub.html&COLL=S&LEG=3&NR=1413&VOLGNR=1&LANG=fr>)

qué ci-avant - l'Autorité estime qu'il est souhaitable d'**habiliter le Roi à « arrêter [périodiquement], après vérification du besoin opérationnel et du respect des conditions⁵⁵, la liste des responsables du traitement autorisés à équiper les membres de leur personnel de caméras individuelles »** .

57. En tout état de cause, il n'est pas admissible que – comme le Projet le prévoit pour les unités opérationnelles de la protection civile⁵⁶ - la demande d'autorisation puisse être adressée à un **délégué du Ministre**. En effet, ce libellé est susceptible d'être interprété comme permettant au responsable du traitement de s'adresser une demande d'autorisation à lui-même.

II.7. Règles d'activation et d'utilisation

58. L'Autorité accueille favorablement la précision (répétée à divers endroits de l'exposé des motifs) suivant laquelle l'activation de la caméra « *ne peut en aucun cas se traduire par une captation continue des images et du son pendant toute la durée d'une mission ou d'un service. Cette limitation découle de la nature même de la caméra individuelle, qui constitue un outil destiné à être utilisé dans le cadre d'interventions spécifiques et non un instrument de surveillance permanente de l'espace public ou des personnes* ».
59. L'Autorité estime cependant que le terme « *permanente* » devrait être supprimé⁵⁷. En effet, **la surveillance (même temporaire) de l'espace public ou des personnes n'est pas compatible avec les finalités énumérées par le Projet**.
60. De plus, l'Autorité estime que les auteurs du Projet devraient envisager l'opportunité d'**énumérer certains lieux où les caméras individuelles ne peuvent être activées que sur demande de la personne concernée** (par exemple les lieux privés ou les lieux sensibles⁵⁸, pour les porteurs susceptibles d'accéder à de tels lieux⁵⁹) et les personnes qu'il convient d'éviter de filmer dans la mesure du possible (très jeunes enfants, victimes secourues⁶⁰, etc...). L'Autorité ne considère pas qu'une interdiction devrait nécessairement viser l'ensemble des lieux et des personnes cités en exemple ci-avant, mais estime que **le caractère nécessaire et proportionné de l'activation d'une caméra individuelle, dans ces lieux ou face à ces catégories de personnes, devrait à tout le moins être démontré avec une attention toute particulière**, dans les commentaires des articles du

⁵⁵ Par le biais d'évaluations et d'audits.

⁵⁶ A l'art. 12/1, §2, *in fine* nouveau de la loi caméras.

⁵⁷ De la dernière phrase du paragraphe.

⁵⁸

⁵⁹ Tels que les services opérationnels de la sécurité civile ;

⁶⁰ Par exemple, la victime justifiant l'intervention des services opérationnels de la sécurité civile.

Projet. A noter qu'il pourrait être prévu que l'avis des conseils communaux (recommandé *supra*) porte également sur cet aspect.

61. L'Autorité accueille tout aussi favorablement l'obligation de faire précéder l'activation d'une caméra individuelle d'un **avertissement** oral⁶¹. Elle estime cependant que les **exceptions**⁶² à cette règle **sont exprimées de manière trop générales**. Bien entendu, l'Autorité admet que « *la sécurité du porteur de la caméra individuelle ou des personnes présentes* » est une préoccupation importante et légitime. Toutefois, il existe des circonstances où c'est l'activation qui sera susceptible de mettre en danger « *la sécurité du porteur de la caméra individuelle ou des personnes présentes* »⁶³. Par conséquent, il convient également de prévoir que « *la caméra individuelle ne peut pas être activée lorsque son activation est susceptible de mettre la sécurité du porteur en danger* ».
62. En ce qui concerne l'**impraticabilité justifiée par le nombre de personnes à avertir**, l'Autorité estime qu'il convient de tenir compte du fait que l'avertissement peut, à lui seul, avoir un effet de désescalade et que le nombre de personnes à avertir ne peut dispenser le porteur d'avertir de l'activation d'une manière qui soit audible pour les personnes les plus proches⁶⁴.
63. L'impraticabilité justifiée par le **danger immédiat de la personne à avertir** conduit à s'interroger sur l'aptitude de l'activation d'une caméra à écarter ce danger immédiat. Cependant, si un tel cas de figure est dûment exemplifié dans le commentaire de l'article concerné, l'Autorité considère que cette exception peut être admise. A l'inverse, si la personne à prévenir est dans un état de conscience altéré, l'avertissement ne sera pas impraticable. Il pourrait tout au plus s'avérer inutile. Toutefois, dans la mesure où cette inutilité n'apparaîtra avec certitude qu'*a posteriori*, l'Autorité considère que l'obligation d'avertissement doit être maintenue dans cette hypothèse.
64. Enfin, l'avertissement « **manifestement inappropriée ou inutile, en particulier lorsque la caméra individuelle est utilisée à un endroit dépourvu de présence humaine** », ne devrait être **applicable qu'aux services opérationnels de la sécurité civile**. Il convient donc de le préciser dans le Projet.
65. L'Autorité insiste pour que ces modifications soient accompagnées de l'obligation pour les caméras utilisées d'être équipées d'un **avertissement lumineux visible** indiquant que la caméra est active

⁶¹ Art. 12/1, §3 nouveau, 12/2, §3 nouveau et 13/14, al. 2 nouveau.

⁶³ Le fonctionnaire délégué indique d'ailleurs à cet égard que « *le risque évoqué ne peut naturellement pas être exclu dans une situation individuelle. L'effet de l'utilisation d'une caméra individuelle dépend notamment des circonstances de l'intervention et de la manière dont son activation est annoncée* ».

⁶³ Le fonctionnaire délégué indique d'ailleurs à cet égard que « *le risque évoqué ne peut naturellement pas être exclu dans une situation individuelle. L'effet de l'utilisation d'une caméra individuelle dépend notamment des circonstances de l'intervention et de la manière dont son activation est annoncée* ».

⁶⁴ Sans préjudice de l'avertissement lumineux dont il sera question *infra*.

et qu'un enregistrement est en cours. Il s'agit d'ailleurs là d'une exigence classique dans les juridictions ayant admis le port de caméras individuelles⁶⁵.

66. L'Autorité accueille également favorablement le fait que les éléments minimaux permettant de répondre à l'obligation de transparence soient prévus⁶⁶. L'Autorité estime cependant que la politique relative à la vie privée rappelant la possibilité d'exercer son droit d'accès et/ou d'introduire un recours auprès de l'APD ainsi que les règles d'utilisation des caméras, doit pouvoir être **consultable**, sur simple demande, **sur les lieux** où les caméras individuelles sont portées. Lorsqu'un accès en ligne est proposé (par exemple via un QR code), il convient de tenir compte de la fracture numérique⁶⁷ et d'imposer aux membres du personnel équipés de caméras individuelles de disposer en tout temps (sinon sur eux, au moins dans le véhicule) d'une version papier de ce document. Il convient donc de modifier le Projet en ce sens.
67. La **fonctionnalité de pré-enregistrement** imposée par le Projet constitue également une garantie très importante aux yeux de l'Autorité. Le fonctionnaire délégué précise d'ailleurs que la notion d' « *objectivation* » des interactions ou celle de « *constatation objective du déroulement d'incidents* » résulte « *notamment de la fonction de pré-enregistrement : lorsque la caméra est activée, la séquence issue du pré-enregistrement est automatiquement ajoutée au début de l'enregistrement effectif. Cette fonction permet de restituer le contexte dans lequel l'intervention débute* ».
68. Afin de ne pas verser dans la surveillance permanente, le Projet prévoit logiquement que l'enregistrement résultant de la captation continue est écrasé après 30 secondes et que ce n'est qu'en cas d'activation (pour l'une des finalités du Projet) que la séquence issue du pré-enregistrement est adjointe à

⁶⁵ Voy. l'ICO guidance on Body Worn Video (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/body-worn-video-bwv/>)

⁶⁶ Art. 12/1, §4 *nouveau* de la loi caméras: « La décision [d'utilisation de caméras individuelles] fait l'objet d'une information du public. À cette fin, le responsable du traitement publie, sur son site internet officiel, une information relative à l'existence du recours aux caméras individuelles ainsi qu'aux principales règles encadrant leur utilisation, en particulier les finalités poursuivies, les conditions d'activation et les garanties en matière de protection des données ». Une disposition à peu près similaire figure aux art. 13/6, §5 et 13/14, al. 3 de la loi relative à la Sécurité civile.

⁶⁷ Ainsi que la Cour Constitutionnelle l'a mis en évidence dans son arrêt [n°126/2025](#), la fracture numérique existe toujours. En témoigne également la [réclamation](#) collective introduite le 28 septembre 2026 contre l'Etat belge pour dénoncer les inégalités entraînées par la digitalisation des services publics et privés ; voy. également à cet égard le [rapport](#) de la Fondation Roi Baudouin « Inclusion numérique, Baromètre de l'inclusion numérique, 2022 », l'[étude](#) 2022 de l'Association belge de recherche et d'expertise des organisations de consommation « Réduire la fracture numérique pour l'ensemble des consommateurs dans la société » ainsi que l'[avis](#) relatif à l'impact de la digitalisation des services (publics ou privés) rendu le 3 février 2023 par Unia et le Service de lutte contre la pauvreté, la précarité et l'exclusion sociale ; voy. en outre l'arrêt [n° 106/2004](#) ayant annulé les dispositions législatives qui prévoyaient que le Moniteur belge ne serait plus publié que sur Internet et non plus en version papier (hormis trois exemplaires). La Cour a jugé que cette mesure introduisait « une différence de traitement entre celui qui, ayant accès à un matériel informatique, peut consulter aisément tous les numéros du Moniteur belge édités depuis la mise en vigueur des dispositions attaquées et y trouver le texte qui l'intéresse, et celui qui, n'ayant pas accès à l'informatique, ne peut identifier le numéro dans lequel ce texte est publié » et que « Faute d'être accompagnée de mesures suffisantes qui garantissent un égal accès aux textes officiels, la mesure attaquée a des effets disproportionnés au détriment de certaines catégories de personnes et n'est dès lors par compatible avec les articles 10 et 11 de la Constitution » ; dans le même sens, voy. l'arrêt [n° 10/2007](#).

l'enregistrement effectif et conservée⁶⁸. L'Autorité ne remet aucunement en question la pertinence de la fonctionnalité de pré-enregistrement, mais estime que, dans la mesure où l'activation de la caméra individuelle détermine le contenu de ce pré-enregistrement, il n'est pas approprié de qualifier les données issues de cet enregistrement d'« *objectives* ». L'Autorité estime que si ce terme devait être maintenu dans le Projet, l'exposé des motifs et le commentaire des dispositions concernées, il convient de le mettre entre guillemets et de **mentionner le fait que le moment de l'activation de la caméra influence le contenu du pré-enregistrement, dans le commentaire de l'article concerné**.

II.8. Destinataires des données et enregistrements

69. Tout d'abord, l'Autorité constate que l'art. 8 du Projet limite l'accès aux données et enregistrements aux seules personnes désignées par le responsable du traitement. L'Autorité comprend que cette disposition vise l'accès par les membres de son personnel. Il serait toutefois préférable de clarifier cette notion d'accès dans le Projet. A cet égard, les membres du « *personnel, chargés de la formation ou de l'accompagnement professionnel ou de l'amélioration des processus de sécurité et désignés par le responsable du traitement* » ne devraient pas être considérés comme des destinataires (puisque'il s'agit de préposés du responsable du traitement). L'Autorité signale au passage qu'elle accueille favorablement le fait qu'il soit prévu dans le Projet que les données traitées dans le cadre de cette finalité doivent au minimum avoir été préalablement pseudonymisées.
70. De plus, ce même art. 8 mentionne des *accès directs* ou *indirects*, sans toutefois définir ces notions. Outre la nécessité de définir ces notions, l'Autorité estime que cette désignation doit reposer sur des règles contraignantes dont le respect doit pouvoir être vérifié et qu'il convient que la disposition en projet impose aux responsables du traitement d'**établir une politique d'accès**, au titre de condition permettant au responsable du traitement de figurer dans l'AR énumérant les responsables du traitement autorisés à utiliser des caméras individuelles⁶⁹.
71. L'Autorité ajoute que le Projet doit également imposer, toujours au titre de condition permettant au responsable du traitement d'utiliser des caméras individuelles, que « *toute personne qui n'est pas légalement tenue au secret professionnel et qui a accès aux images et aux sons, ainsi qu'aux données GPS, est soumise à un devoir de discrétion ou à une **obligation contractuelle de confidentialité** dont le non-respect doit être assorti de **sanctions dissuasives*** »⁷⁰.

⁶⁸ Voy. notamment l'art. 28 du Projet.

⁶⁹ A propos de cette habilitation au Roi, voy. *supra*.

⁷⁰ L'art. 13/10 de la loi de 2007 relative à la sécurité civile est libellé de manière analogue, mais ne mentionne pas l'obligation contractuelle de confidentialité (qu'il est nécessaire de prévoir pour le personnel du secteur privé), ni le caractère dissuasif des sanctions encourues.

72. En ce qui concerne les (autres) destinataires énumérés par cet article 8, plusieurs questions se posent. Ainsi, en ce qui concerne les membres des **services de police et les autorités judiciaires**, soit il s'agit de permettre au porteur et/ou au responsable du traitement de déposer une plainte pénale et dans ce cas, cette disposition est légitime, soit il s'agit de permettre aux membres des services de police et aux autorités judiciaires de réclamer ces données, informations et enregistrements au responsable du traitement, pour des besoins liés à une enquête visant une personne dont les données figurent dans le registre, pour des faits étrangers à toute plainte du porteur et/ou du responsable du traitement (par exemple, pour permettre d'identifier les personnes présentes à un endroit précis)⁷¹.
73. En ce qui concerne cette seconde hypothèse, l'Autorité accueille favorablement le fait que le registre n'est appelé à contenir **aucune donnée d'identification** relative à la personne filmée, que l'art. 7 **interdit** l'utilisation des caméras individuelles et des logiciels associés pour **l'authentification ou l'identification biométrique** et que le commentaire de cette disposition **interdit** tout **couplage**⁷² avec des bases de données à caractère personnel. En effet, en disposer autrement aurait inmanquablement conduit à mettre en œuvre un mécanisme de surveillance disproportionné. Cependant, afin de conférer un véritable effet utile à ces interdictions, l'Autorité estime qu'il convient de **préciser que « le respect de ces interdictions par les éventuels destinataires est une condition sine qua non de la communication de ces données »**. Une exception à cette interdiction de communication pourrait toutefois être prévue (sans préjudice de l'avis du COC), dans le respect du principe de proportionnalité⁷³ et à condition que le cadre légal applicable au destinataire en question autorise ce dernier à effectuer des traitements de données biométriques.
74. Il doit en outre **être veillé à ce que le port de caméras individuelles ne conduise jamais à différer une intervention policière** sous prétexte que les auteurs de faits ont pu être filmés, car, comme l'indiquait le fonctionnaire délégué, *« c'est la combinaison de ces différents instruments, adaptée aux circonstances concrètes, qui est susceptible d'apporter une réponse appropriée »*.
75. L'Autorité estime qu'il appartient à l'auteur du projet de démontrer le caractère nécessaire et proportionné de la possible communication des données du registre (en ce compris les enregistrements) aux membres des services de police agissant dans le cadre de leurs **compétences en matière de police administrative**.

⁷¹ Ce qui - sans préjudice de ce qui est dit ci-dessous - pourrait également être admis dans une série limitée de cas (p.ex. dans le cadre d'une instruction judiciaire concernant des crimes susceptibles d'entraîner les peines de réclusion les plus élevées), tout en gardant à l'esprit que la limitation des possibilités d'exploitation des enregistrements constitue également une mesure de protection des porteurs (dont il ne faut pas oublier qu'ils ne sont pas membres des services de police).

⁷² Le Projet ajoute « en temps réel », mais le fonctionnaire délégué a précisé que *« les auteurs du projet n'entendent pas consacrer, par cette formulation, une possibilité spécifique de couplage a posteriori. La référence au temps réel vise à préciser que la caméra individuelle ne peut être utilisée, pendant son utilisation, comme un outil permettant une confrontation automatisée avec des bases de données externes »*.

⁷³ P.ex. dans le cadre d'une instruction judiciaire concernant des crimes susceptibles d'entraîner les peines de réclusion les plus élevées, évoqué ci-avant.

II.9. Possibilité de limiter les droits des personnes concernées

76. L'art. 5 du Projet dispose que « *toute personne dont les données audiovisuelles sont captées dispose d'un droit d'accès aux données audiovisuelles* », mais ajoute que ce droit peut être temporairement limité dans les cas prévus à l'art. 23.1.c et d du RGPD.
77. Si une telle limitation peut se comprendre pour les services de police⁷⁴, la **nécessité d'une telle limitation** pour des porteurs non-policiers apparaît nettement moins évidente. Interrogé à ce sujet, le fonctionnaire délégué a précisé que « *la nécessité d'une telle limitation ne dépend pas de l'existence de pouvoirs de police dans le chef du service qui a réalisé l'enregistrement, mais de la nature des images enregistrées et des circonstances dans lesquelles l'accès est demandé. Ainsi, des images enregistrées par un service non policier peuvent ultérieurement présenter un intérêt pour une enquête administrative ou judiciaire. Leur communication immédiate pourrait, par exemple, porter atteinte aux droits de tiers ou compromettre le bon déroulement d'une enquête en cours* ».
78. Comme l'Autorité l'indiquait dans son avis n° [114/2023](#)⁷⁵ précité « *même en cas d'utilisation [des enregistrements] 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* ». Il pourrait en revanche être prévu que « *si les faits enregistrés font l'objet d'une enquête judiciaire, la **demande d'accès** par une personne concernée, adressée au responsable du traitement est **transférée sans délai au parquet ou au juge d'instruction en charge de l'enquête ou de l'instruction** et l'accès ne peut être temporairement refusé que si ces derniers s'opposent expressément à cet accès dans un délai de 5 jours* ». Cette possibilité est admissible en raison des garanties entourant ce type d'enquête (et en particulier de l'intervention d'un magistrat indépendant). Dès lors que ces garanties sont inexistantes dans le cas des enquêtes administratives ou disciplinaires, la possibilité de limitation de l'accès ne peut leur être étendue.
79. Ceci étant dit, indépendamment d'une enquête, **l'Autorité admet qu'une communication immédiate soit susceptible de porter atteinte aux droits de certains tiers** (victimes, témoins, personnes vulnérables voire collègues du porteur). Il s'agit donc de trouver un juste équilibre permettant d'assurer que les caméras individuelles restent un outil au service de la transparence des interventions (et que la documentation « *aussi complètement que possible [du] déroulement factuel de l'intervention* » qu'évoquait le fonctionnaire délégué⁷⁶ ne soit pas uniquement admise lorsqu'elle intervient « à

⁷⁴ Qui, pour rappel, ne sont pas visés par le présent Projet.

⁷⁵ Point 60.

⁷⁶ Voy. *supra*.

charge ») et ne se mue pas en un outil de surveillance. L'Autorité estime que cet équilibre peut être atteint **en remplaçant la communication immédiate par une consultation de l'enregistrement dans les locaux du responsable du traitement, lorsque la remise d'une copie de l'enregistrement est susceptible de porter atteinte aux droits de certains tiers**. Enfin, comme indiqué *supra*, il est **indispensable de prévoir que les logiciels des caméras individuelles doivent disposer de capacités de floutage/masquage, permettant de garantir un droit d'accès dans le respect des droits des tiers**⁷⁷.

II.10. Mesures de sécurité applicables

80. Les caméras individuelles sont des appareils mobiles captant à la fois des images et du son (donc enregistrant notamment des visages et des voix), pouvant être portés de différentes manières, mais qui sont susceptibles d'être détruits, perdus ou volés durant une altercation⁷⁸. De plus, certains modèles de caméras prévoient un accès à distance (wifi, bluetooth, etc.), ce qui expose les données qui y sont contenues à des vulnérabilités très importantes et peut même dans certains cas permettre de suivre les déplacements des porteurs⁷⁹. Par ailleurs, en raison de l'immense quantité de données que le recours à ce type de caméras impose de stocker, il est souvent nécessaire de faire appel à des fournisseurs de services cloud externes. Ceci est susceptible d'exposer les données à des transferts internationaux et/ou à les soumettre à des législations étrangères incompatibles avec le RGPD⁸⁰.
81. Dans un contexte où les cyberattaques sont appelées à se multiplier et à devenir de plus en plus sophistiquées en raison des progrès de l'intelligence artificielle⁸¹ et du développement de l'informatique quantique, l'Autorité se doit de faire preuve d'une plus grande exigence en matière de minimisation des données et de mesures techniques et organisationnelles à mettre en place pour garantir un haut

⁷⁷ En ce sens, voy. l'ICO guidance on Body Worn Video, *op. cit.* ; voy. également DPC Guidance on the use of Body Worn Cameras or Action Cameras, p. 6

(https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Body%20Worn%20Cameras%20or%20Action%20Cameras_Jan20.pdf)

⁷⁸ Peter Hermann, "D.C. Poised to Test Body Cameras for Police Officers," Washington Post, September 6, 2014, accessed January 10, 2015

(http://www.washingtonpost.com/local/crime/dc-poised-to-test-body-cameras-for-police-officers/2014/09/06/358ebc52-3459-11e4-a723-fa3895a25d02_story.html), cité par Alexandra Mateescu, Alex Rosenblat and Danah Boyd, Working Paper on Police-Worn Cameras, Data&Society Research Institute, Feb. 2015, p. 5

(<https://datasociety.net/wp-content/uploads/2015/10/PoliceBodyWornCameras-1.pdf>); voy. également Home Office, Safeguarding Body Worn Video Data, Publication No.011/18, Oct. 2018, pp. 14 et sv. (<https://assets.publishing.service.gov.uk/media/5bb769f6ed915d23b3cabd20/safeguarding-body-worn-video-data-01118p.pdf>)

⁷⁹ Voy. <https://www.abc.net.au/news/2026-05-04/police-location-tracked-bluetooth-flaw-axon-tasers-bodycams/106610886> et <https://azmirror.com/2020/07/02/fort-huachuca-police-body-cam-footage-easily-accessible-after-an-ebay-purchase/>; voy. également D. Oberhaus, Hackers Can Edit Police Body Cam Footage Without Anybody Noticing, Vice 13.08.2018 (<https://www.vice.com/en/article/hackers-can-edit-police-body-cam-footage-without-anybody-noticing/>);

⁸⁰ Voy. <https://securityaffairs.com/81935/digital-id/german-police-bodycam-amazon-servers.html>.

⁸¹ <https://www.staysafeonline.org/fr/articles/pourquoi-votre-famille-et-vos-coll%C3%A8gues-ont-besoin-d-un-mot-de-passe-dans-l-%C3%A8re-de-l-ia>

niveau de cybersécurité, lorsque de nouveaux traitements de données - tels que l'enregistrement de voix⁸² - sont susceptibles d'engendrer des risques accrus en la matière.

82. En l'espèce, l'Autorité craint qu'alors que les pouvoirs publics sous-investissent déjà dans la cybersécurité⁸³, les entreprises commerciales autorisées à équiper certains membres de leur personnel de caméras individuelles soient tentées de limiter au maximum les investissements nécessaires dans une technologie permettant d'atteindre le niveau de sécurité des données requis pour traiter des données présentant un degré (potentiellement) élevé de sensibilité⁸⁴.
83. De plus, dans le contexte belge où les autorités publiques ne peuvent se voir infliger des amendes par la Chambre contentieuse de l'Autorité et où la jurisprudence de la Cour des marchés ne lui permet pas d'infliger des amendes dissuasives aux entreprises privées, l'Autorité estime qu'il **serait irresponsable d'autoriser des responsables du traitement à équiper les membres de leur personnel de caméras individuelles sans les soumettre à des conditions minimales de sécurité**⁸⁵, par le biais d'une politique de sécurité contraignante adoptée et tenue à jour par les services du Ministre de la Sécurité et de l'Intérieur⁸⁶, dont le respect serait attesté par un audit périodique, au titre de condition permettant à ces responsables du traitement de figurer ou de maintenir leur présence dans la liste arrêtée par le Roi⁸⁷.
84. L'Autorité estime par ailleurs qu'il est indispensable de prévoir dans le Projet que ces conditions minimales de sécurité comportent l'obligation, pour l'autorité ou l'entreprise candidate au déploiement de caméras individuelles, de **disposer d'un responsable de la Sécurité des Systèmes d'Information (CISO) titulaire d'un diplôme de master en cybersécurité**.
85. De plus, l'Autorité estime que **l'existence de voies de recours ne constitue pas une garantie suffisante** pour le rétablissement des droits des utilisateurs dont les données feraient l'objet d'un accès illégitime (par des membres du personnel ou par un tiers qui profiterait d'une faille de sécurité) ou d'un détournement de finalité. Par conséquent, l'Autorité estime que, pour ces situations, il convient de prévoir l'initiation d'une **procédure visant à rétablir la personne concernée dans ses droits**

⁸² <https://www.bbc.com/future/article/20260804-why-your-family-needs-a-secret-codeword>

⁸³ <https://www.vrt.be/vrtnws/nl/2024/01/19/gegevens-hack-limburg-net/>; <https://www.vrt.be/vrtnws/nl/2022/11/24/hacking-politie-zwijndrecht/>

⁸⁴ Comme cela a été constaté dans l'autres domaines, p. ex. <https://www.computable.be/2024/12/18/forse-boete-voor-ziekenhuis-wegens-gebrekkige-it-beveiliging/> et <https://www.lalibre.be/belgique/societe/2022/05/27/cyberattaque-chez-vivalia-une-digitalisation-trop-rapide-pourrait-expliquer-la-fragilite-des-hopitaux-MG5OBCUJSZGXVNEVAXNOSAURM/>

⁸⁵ Que le responsable du traitement conserve bien entendu la liberté de doubler d'une politique de sécurité interne plus contraignante.

⁸⁶ Voy. p. ex. Federal Bureau of Investigation, U.S. Department of Justice. Criminal Justice Information Services (CJIS) Security Policy. Version 5.9.4. 20 Dec. 2023, https://le.fbi.gov/file-repository/cjis_security_policy_v5-9-4_20231220.pdf.

⁸⁷ Sur cette question voy. *supra*.

– indépendante de l’initiative de la personne concernée – ainsi que l’indemnisation de la personne concernée.

86. Il convient par ailleurs de prévoir que, lors de la commande des caméras individuelles, les responsables du traitement doivent **imposer contractuellement** (via les clauses administratives du cahier spécial des charges pour les autorités publiques) **à leurs fournisseurs qu’« en cas d’accès irrégulier résultant de l’exploitation d’une faille de sécurité des produits fournis (en ce compris les logiciels), sans préjudice du droit des personnes concernées d’engager la responsabilité de la partie contrevenante, le fournisseur sera redevable de plein droit, envers chacune des personnes concernées par la fuite de ses données, d’un montant forfaitaire indexé de 3.000 EUR »**.
87. L’Autorité ajoute que la politique de sécurité édictée au niveau du SPF Intérieur devra veiller à imposer un **chiffrement robuste** et l’établissement d’une **stratégie permettant d’évoluer vers des standards de chiffrements dits « post-quantiques »**⁸⁸, à imposer l’implémentation d’une solution technique permettant un **effacement automatique** des données après 30 jours, sous réserve d’une manipulation spécifique permettant de prolonger la conservation pour 90 jours maximum lorsque les conditions d’une telle prolongation sont remplies⁸⁹, à permettre d’associer des métadonnées de **géolocalisation** aux enregistrements, mais pas de diffuser ces données en direct (sauf pour les services opérationnels de la sécurité civile⁹⁰) et à **interdire la possibilité d’activation automatique**⁹¹ en raison des risques de dysfonctionnement qu’elle implique⁹².

⁸⁸ Sur cette question voy. https://cybersecuritycoalition.be/wp-content/uploads/CSC-WP-PQC-Vol1_FINAL.pdf

⁸⁹ Ceci constitue en effet une garantie efficace contre l’oubli d’effacement.

⁹⁰ Sous réserve de ce qui a été dit *supra*.

⁹¹ Voy. Scientific Working Group on

Digital Evidence, Considerations for Body Worn Camera Systems, SWGDE 23-V-002-1.0, point 6.8. (<https://www.swgde.org/wp-content/uploads/2026/03/2026-02-25-Considerations-for-Body-Worn-Camera-23-V-002-1.0.pdf>).

⁹² Voy. le chapitre intitulé “Concerns regarding their own privacy”, dans Poirier, B., Charbonneau, É., & Boivin, R. (2024). Police body-worn cameras and privacy: Views and concerns of officers and citizens. *International journal of police science & management*, 26(2), 170–181. <https://doi.org/10.1177/14613557231214383>, où une utilisatrice interrogée déclare: “Me, personally, I always take off my bulletproof vest [on which BWCs are attached] when I go to the bathroom, so that kind of thing won’t happen to me. But it happened to one of my colleagues, and she wasn’t thrilled. She was like, “Will it be erased?”. Well, no, it stays in the cloud. (User/end of pilot; female officer with 9 years of police experience)”.

PAR CES MOTIFS,**L'Autorité est d'avis que**

1. Les raisons pour lesquelles le « port » d'une caméra individuelle, par un service, peut être autorisé doivent être distinguées des finalités d'« activation » de la caméra (**considérant n°28**) ;
2. La finalité relative à la protection de la sécurité « *des agents* » ne devrait viser que « *l'agent porteur* » (**considérant n°29**) ;
3. Une hiérarchie des finalités doit être établie (**considérant n°30**) ;
4. Il convient de relativiser le terme « *objective* » utilisé pour qualifier les constatations d'incidents au moyen de caméras individuelles (**considérants n°31-32 et 68**) ;
5. La référence au seul objectif de traiter des catégories particulières de données est à proscrire (**considérant n°34**) ;
6. Le Projet doit comporter des exigences minimales en matière de possibilité d'édition des enregistrements et les auteurs du Projet devraient envisager l'opportunité d'énumérer certains lieux où les caméras individuelles ne peuvent être activées que sur demande de la personne concernée (**considérants n°35, 60 et 79**) ;
7. Les finalités liées à la répression des comportements des tiers ou des porteurs et de support pédagogique ne sont pas susceptibles de justifier une ingérence aussi étendue que les finalités liées à la protection de l'intégrité physique des intervenants (**considérant n°37**) ;
8. Le Projet devrait prévoir que lorsqu'un agent porteur fait l'objet de comportements agressifs, il peut activer sa caméra individuelle « *les porteurs doivent être formés à s'abstenir d'activer leur caméras lorsqu'un avertissement préalable a permis d'atteindre l'objectif de désescalade du conflit* » (**considérant n°38**) ;
9. Le Projet doit distinguer les finalités de traitement des données GPS ne pouvant pas justifier une communication (ou un accès) en temps réel de celles qui sont susceptibles de la justifier (**considérant n°40**) ;
10. Il convient de justifier la raison pour laquelle il est nécessaire que ces données de géolocalisation soient transmises en temps réel via la caméra (**considérants n°41-42**) ;
11. Les fonctionnalités d'enregistrement des images et du son ainsi que la communication en temps réelle doivent pouvoir être activées et désactivées par le porteur (sur base d'une politique contraignante) (**considérant n°43**) ;
12. Le caractère proportionné de la mesure peut être démontré dans le cadre d'une phase test limitée à deux ans et l'obligation de faire réaliser une étude (universitaire) indépendante dans ce délai (**considérants n°45-50**) ;

- 13.** Le Roi devrait être habilité à arrêter (par exemple tous les deux ans), après vérification du besoin opérationnel et du respect des conditions, la liste des responsables du traitement autorisés à équiper les membres de leur personnel de caméras individuelles (**considérant n°51 et 54-56**) ;
- 14.** Il n'est pas admissible de libeller une disposition en des termes permettant au responsable du traitement de s'adresser une demande d'autorisation à lui-même (**considérant n°57**) ;
- 15.** La surveillance (même temporaire) de l'espace public ou des personnes n'est pas compatible avec les finalités énumérées par le Projet (**considérant n°59**) ;
- 16.** Les exceptions à l'avertissement oral préalable à l'activation devraient être fortement limitées (**considérants n°61-64**) ;
- 17.** Une obligation d'équiper les caméras utilisées d'un avertissement lumineux visible indiquant que la caméra est active et qu'un enregistrement est en cours doit être prévue (**considérant n°65**) ;
- 18.** La politique relative à la vie privée rappelant la possibilité d'exercer son droit d'accès et/ou d'introduire un recours auprès de l'APD ainsi que les règles d'utilisation des caméras, doit pouvoir être consultable, sur simple demande, sur les lieux où les caméras individuelles sont portées (**considérant n°66**) ;
- 19.** Les conditions permettant au responsable du traitement d'être mentionné dans l'AR énumérant les responsables du traitement autorisés à utiliser des caméras individuelles doivent inclure l'adoption d'une politique d'accès et l'obligation de soumettre toute personne qui n'est pas légalement tenue au secret professionnel et qui a accès aux images et aux sons (ainsi qu'aux données GPS si applicable), à un devoir de discrétion ou à une obligation contractuelle de confidentialité dont le non-respect doit être assorti de sanctions dissuasives (**considérants n°70-71**) ;
- 20.** Les interdictions d'effectuer des traitements de données biométriques et de couplage des enregistrements doivent être étendues aux destinataires (**considérants n°72-74**) ;
- 21.** Le caractère nécessaire et proportionné de la possible communication des données du registre (en ce compris les enregistrements) aux membres des services de police agissant dans le cadre de leurs compétences en matière de police administrative doit être démontrée (**considérant n°75**) ;
- 22.** Les possibilités de limitation d'exercice des droits devraient être tempérées (**considérants n°77-79**) ;
- 23.** Il serait irresponsable d'autoriser des responsables du traitement à équiper les membres de leur personnel de caméras individuelles sans les soumettre à des conditions minimales de sécurité (**considérants n°80-83 et 87**) ;
- 24.** Les conditions minimales de sécurité doivent inclure l'obligation de disposer d'un CISO titulaire d'un diplôme de master en cybersécurité (**considérant n°84**) ;

25. Une procédure visant à rétablir la personne concernée dans ses droits ainsi que son indemnisation automatique et forfaitaire doivent être prévues (**considérants n°85-86**).

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice