Paris, le 11 mars 2022

A :	**Commission Nationale de l'Informatique et des Libertés (CNIL)**
De :	**PERIFEM**
Objet :	**Réponse à consultation – Projet de position relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics**
Date :	**11 mars 2022**

PERIFEM soutient l'initiative de la CNIL de prendre position sur les conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, et de poser les bases d'un débat démocratique en soumettant sa position à consultation publique.

Cette initiative est une première étape vers une sécurité juridique accrue, dont l'écosystème de la vision par ordinateur a besoin pour se développer de manière pérenne et responsable, et accroitre ainsi la souveraineté française et européenne en la matière.

Si, comme la CNIL, PERIFEM considère que des mesures législatives et réglementaires spécifiques seraient de nature à accroître la sécurité juridique, PERIFEM considère qu'à droit constant, le cadre légal actuel permet déjà le déploiement de nombreux cas d'usages de dispositifs de vidéo intelligente.

I N T R O D U C T I O N

PERIFEM salue et soutient l'initiative de la CNIL de prendre position sur les conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, et de soumettre sa position à consultation publique. Cette démarche fait de la CNIL l'autorité de protection des données pionnière dans l'Union Européenne en matière de technologie de vision par ordinateur (*computer vision*).

PERIFEM représente de nombreuses enseignes françaises de la grande distribution, du commerce spécialisé et des centres commerciaux, ainsi que des startups françaises concevant des solutions de caméras intelligentes, et contribue au partage d'informations, au défrichage d'innovations et à l'élaboration des réglementations depuis sa création en 1980.

PERIFEM et ses membres soutiennent le déploiement et l'usage responsable des caméras intelligentes dans les commerces (hors reconnaissance faciale).

Plus largement, ils sont mobilisés sur le sujet de la sécurité et encouragent l'utilisation de nouvelles technologies pour contribuer à la lutte contre le vol en magasin, qui est à l'origine, en France, d'une perte annuelle de chiffre d'affaires estimée à environ 7 milliards d'euros[1], perte qui impacte directement les prix exercés par les commerçants, et ainsi le pouvoir d'achat des Français.

PERIFEM accueille positivement la volonté de la CNIL de faire évoluer le cadre législatif et règlementaire existant afin d'accroître la sécurité juridique dans le cadre de l'emploi de caméras intelligentes. En cela, PERIFEM partage la conviction de la CNIL qu'un cadre juridique clair et prévisible est une condition nécessaire au développement de technologies françaises et européennes compétitives et respectueuses des droits et libertés des individus dès leur conception.

[1] Chiffre 2017 - https://www.crimetech.it/landing/retail-security-in-europe/Retail-Security-in-Europe-Executive-Summary-EN.pdf

PERIFEM entend, par la présente réponse à consultation, formuler des commentaires et suggestions de rédaction relatifs au projet de position de la CNIL sur les conditions de déploiement des caméras intelligentes dans les espaces publics, en se concentrant sur les aspects suivants :

- **Parties 1, 2 et 3** : l'objectivisation des sentiments de surveillance généralisée et d'analyse généralisée associés à la vidéoprotection et aux vidéos intelligentes, et des propositions afin de renforcer l'information des personnes concernées sur les dispositifs de vidéo intelligente mis en œuvre ;
- **Partie 4** : l'analyse de la conformité de certains dispositifs de vidéo intelligente aux principes généraux du RGPD et, tout particulièrement au droit d'opposition. Si PERIFEM considère qu'une mesure législative spécifique écartant le droit d'opposition dans certains cas d'usages serait de nature à accroître la sécurité juridique du déploiement des caméras intelligentes, PERIFEM entend exposer qu'à droit constant, des modalités d'exercice conformes au RGPD et à la Loi Informatique et Libertés existent d'ores et déjà.

1. COMMENTAIRES ET SUGGESTIONS SUR LES PARTIES 1 A 3

1.1. COMMENTAIRES SUR LA PARTIE 1

PERIFEM salue le **travail de clarification et de synthèse effectué par la CNIL** afin de définir les technologies de vision par ordinateur, résumer la multiplicité et la diversité des cas d'usages des vidéos intelligentes, et acter de la légitimité et l'utilité d'au moins une partie de ces usages, en particulier dans le commerce de détail.

PERIFEM suggère de souligner dès la première partie de sa position que les technologies de vidéos intelligentes peuvent être utilisées dans de nombreux cas sans impliquer un traitement des données personnelles, pour exclure expressément ces applications de son analyse.

Suggestion de rédaction du paragraphe 1.3. [2]

Si le terme « vidéo augmentée » recouvre une grande variété de solutions, le présent document n'a vocation qu'à traiter des dispositifs, fixes ou mobiles, déployés dans les espaces publics ***opérant un traitement de données personnelles*** *à l'exclusion des dispositifs de reconnaissance biométrique, et notamment des dispositifs de reconnaissance faciale qui font l'objet de problématiques et d'un encadrement spécifique déjà évoqués par la CNIL dans une publication de novembre 2019. Il ne sera pas non plus traité ici des usages de ces dispositifs* ***qui n'impliquent pas la captation et le traitement de données personnelles, ni des dispositifs*** *dans des lieux non ouverts au public (par exemple bureaux, réserves ou entrepôts de magasins...), dans un cadre strictement privé ou encore à des fins de recherche scientifique au sens du RGPD.*

1.2. COMMENTAIRES SUR LES PARTIES 2 ET 3

PERIFEM partage le constat de la CNIL selon lequel *« une appréciation globale de ces dispositifs n'a pas de sens »* (§2.2.7), et qu'une **approche au cas par cas de ces dispositifs**, selon une analyse des **risques gradués** pour les droits et libertés des personne, est la plus adaptée.

[2] Légende : **nos suggestions d'ajouts** en gras souligné / ~~nos suggestions de suppression~~ en barré

Toutefois, PERIFEM souhaite **nuancer la position de la CNIL sur les sentiments de surveillance généralisée et d'analyse généralisée** de la population du fait des déploiements de la vidéoprotection et des vidéos intelligentes, en particulier dans les commerces.

En effet, selon un sondage publié par l'institut OPINION WAY et PERIFEM en mars 2022[3], **77% des Français sont favorables à la vidéosurveillance**[4], et en particulier 86% y sont favorables dans les centres commerciaux, et 84% dans les grandes surfaces alimentaires. Ces chiffres montrent que les Français sont déjà familiers des enjeux associés au déploiement de la vidéosurveillance/vidéoprotection dans les lieux publics qui existe depuis près de 30 ans[5], et surtout, qu'ils y sont très largement favorables dans les commerces.

Selon cette même étude, **plus de 80% des Français accepteraient d'être filmés dans les magasins par des caméras intelligentes pour améliorer la sécurité des personnes et des biens**, et plus de 60% se déclarent favorables à ces technologies afin de faciliter leur expérience en magasin (propreté des espaces, fluidification du passage en caisse par exemple). Là encore, ces chiffres montrent un accueil favorable de l'opinion publique sur ces technologies, dès lors que leur finalité est utile et claire, loin du sentiment de « big brother » relayé par certaines parties prenantes. Cette étude a d'ailleurs été accueillie favorablement par la presse nationale et la radio nationale[6]

Le déploiement responsable des dispositifs de vidéo intelligente doit s'accompagner de garanties fortes, au premier rang desquelles une information précise et complète des personnes concernées. PERIFEM ne partage pas la position de la CNIL sur le fait que le caractère « sans contact » des vidéos intelligentes empêcherait les individus d'avoir conscience que celles-ci peuvent les filmer et les analyser (§3.1.9). La réglementation encadre d'ores et déjà les modalités d'information des personnes concernées s'agissant des systèmes de vidéoprotection ; et PERIFEM considère que les responsables de traitement doivent adapter ces modalités d'information des personnes au caractère novateur des technologies de vision par ordinateur, ce que la CNIL recommande également dans la partie 4 de son projet (§4.2.7.3).

PERIFEM appelle donc les magasins, responsables des traitements, à se mobiliser afin de s'assurer que l'**information est délivrée de manière claire et efficace aux personnes concernées**. A ce titre, PERIFEM propose de mettre en place une charte de bonnes pratiques afin d'harmoniser et de renforcer les pratiques des responsables de traitement du secteur :

- **Sur le fond** : en veillant à ce que l'ensemble des responsables de traitement informent de manière complète et claire leurs clients sur les dispositifs en place dans leurs magasins, en fournissant notamment des modèles de textes à compléter, et en généralisant les doubles niveaux d'informations ;

- **Sur la forme** : en veillant à ce que l'ensemble des responsables de traitement adoptent les supports et les emplacements adaptés, en particulier ceux recommandés par la CNIL : *« panneau d'information, vidéos, codes QR, information sur le site, marquages au sol, annonces sonores... »* (§4.2.7.3)

[3] Etude OPINION WAY – PERIFEM « Vidéosurveillance dans les commerces » - mars 2022 https://www.perifem.com/etude-videosurveillance
[4] La terminologie vidéosurveillance utilisée dans l'étude recoupe la vidéoprotection, les lieux concernés étant des lieux ouverts au public
[5] Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité
[6] Le Figaro - La grande distribution veut développer l'usage de la vidéosurveillance – 8 mars 2022 https://www.lefigaro.fr/societes/la-grande-distribution-veut-developper-l-usage-de-la-videosurveillance-20220308
LSA - Vidéo-surveillance en magasins: les Français votent oui, mais... - 8 mars 2022 https://www.lsa-conso.fr/video-surveillance-en-magasins-les-francais-votent-oui-mais,405316
Europe 1 https://www.europe1.fr/emissions/L-innovation-du-jour/des-cameras-intelligentes-dans-les-magasins-capables-de-detecter-automatiquement-les-vols-4098717

Suggestion de rédaction du paragraphe 3.1.9

3.1.9. Par ailleurs, la vidéo « augmentée » peut constituer une technologie invisible et « sans contact » pour les personnes. Si les citoyens peuvent constater et, d'une certaine manière, appréhender l'installation de différentes caméras vidéo dans leur quotidien, ***les responsables des traitements doivent leur donner les*** ~~*ils n'ont pas de*~~ *moyens d'avoir conscience que celles-ci peuvent, non pas seulement les filmer, mais également les analyser.*

2. COMMENTAIRES ET SUGGESTIONS SUR LA PARTI 4

2.1. COMMENTAIRES SUR LA SECTION 4.1

PERIFEM salue les clarifications apportées par la CNIL sur le champ d'application du **Code de la Sécurité Intérieure (CSI)** qui constitue un premier pas vers une **sécurité juridique accrue** pour les responsables de traitement. En effet, d'une part, le CSI n'a vocation à régir que les dispositifs relevant de son objet de préservation de l'ordre et de la sécurité publics, et ne prohibe pas les dispositifs de vidéo intelligente, et d'autre part, le CSI n'a pas d'effet limitatif sur les dispositifs de vidéo intelligente ne relevant pas de son objet.

2.2. COMMENTAIRES ET SUGGESTIONS SUR LA SECTION 4.2

PERIFEM relève l'effort d'illustration par la CNIL des principes communs du RGPD aux dispositifs de vidéo intelligente, ainsi que les recommandations pratiques proposées en matière de *privacy by design* (§4.2.6.2) et droit à l'information (§4.2.7.3).

S'agissant de la base légale de l'intérêt légitime, la prise de position de la CNIL dans le sens d'une **exclusion de cette base légale dans trois cas de figures particuliers** (§**4.2.5.3**)[7] est étonnante puisque la CNIL ne justifie pas ces exclusions, et celles-ci apparaissent contradictoires avec les principes de la règlementation applicable.

Afin de délimiter plus précisément les contours de ces exclusions, PERIFEM souhaite exposer son interprétation **sur l'analyse au cas par cas de l'intérêt légitime (i) l'application des dispositions relatives au profilage (ii), les limites de la notion de données sensibles au sens du RGPD (iii), et enfin la notion de comportement.**

i. L'intérêt légitime : une base légale nécessitant une analyse au cas par cas

A l'exception des traitements de données sensibles au sens de l'article 9 du RGPD, **l'exclusion de la base légale de l'intérêt légitime pour certaines catégories de traitements est contraire au principe posé par ce**

[7] Projet de position CNIL - §4.2.5.3 « *La CNIL estime ainsi que ne pourraient en principe pas reposer sur l'intérêt légitime :*
- *des dispositifs qui analysent et segmentent les personnes, sur la base de critères tels que l'âge ou le genre afin de leur adresser des publicités ciblées ;*
- *des dispositifs qui analysent et segmentent les personnes sur la base de leurs émotions ou de données sensibles (santé, religion, orientation sexuelle, etc.) ;*
- *des dispositifs qui analysent le comportement et les émotions des personnes sur la base de la détection de leurs gestes et expressions, ou de leurs interactions avec un objet*. »

texte. En effet, le RGPD prône une « *évaluation attentive* »[8] qui doit prendre en compte, **au cas par cas**, les intérêts en présence mais également les garanties pouvant être apportées par le responsable de traitement pour limiter, voire exclure, les incidences sur les individus[9].

C'est également la position du Groupe de travail de l'Article 29 (« G29 ») qui considère que la notion d'intérêt légitime peut inclure des **intérêts très variés**, qu'ils soient futiles ou incontestables, évidents ou plus controversés[10]. L'appréciation de la validité d'un intérêt légitime nécessite une analyse au cas par cas opérant une **mise en balance des intérêts**[11].

ii. Le profilage : un encadrement spécifique et non absolu

Au §4.2.5.3, la CNIL propose d'interdire par principe la base de l'intérêt légitime pour les « *dispositifs qui analysent et segmentent les personnes, sur la base de critères tels que l'âge ou le genre afin de leur adresser des publicités ciblées* », ce qui revient à interdire tous dispositifs de profilage basés sur l'intérêt légitime.

Pourtant, l'article 22 du RGPD prévoit que « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage,* ***produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire*** ».

Comme l'explique le G29, les traitements visés à l'article 22 ne peuvent être basés sur l'intérêt légitime, mais **cette interdiction n'est pas absolue et s'applique uniquement en cas d'effets juridiques ou d'impact significatif sur la personne concernée**[12] :

- La notion de « *décision produisant des effets juridiques* » est explicitée par le G29 comme **affectant les droits légaux d'une personne**, tels que la liberté de s'associer avec d'autres, de voter à une élection ou d'intenter une action en justice, il peut aussi s'agir de conséquences sur le statut juridique d'une personne ou ses droits en vertu d'un contrat[13] ;
- La notion de « *décision affectant de manière significative de façon similaire la personne* » est entendue par le G29 comme ayant un **impact similaire à celui d'une décision produisant un effet juridique**. Ainsi les effets du traitement doivent être « *suffisamment important* » et « *avoir le potentiel de : (i) affecter de* ***manière significative*** *les circonstances, le comportement ou les choix des*

---

[8] RGPD - Considérant 47 : *« l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. »*

[9] CNIL - Fiche sur l'intérêt légitime : comment fonder un traitement sur cette base légale ? *« Ces incidences doivent être mesurées afin de déterminer, au cas par cas, l'ampleur de l'intrusion causée par le traitement dans la vie des personnes. »*

[10] G29 - Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, Page 27

[11] G29 - Avis 06/2014 sur la notion d'intérêt légitime : *« Les facteurs à prendre en considération dans cette mise en balance sont notamment:*
- la nature et la source de l'intérêt légitime, et la question de savoir si le traitement des données est nécessaire à l'exercice d'un droit fondamental, est d'intérêt public à quelque autre égard ou bénéficie d'une reconnaissance dans la collectivité concernée;
- l'incidence sur les personnes concernées et leurs attentes raisonnables quant à ce qu'il adviendra de leurs données, ainsi que la nature des données et la façon dont elles sont traitées;
- les garanties supplémentaires qui pourraient limiter toute incidence injustifiée sur la personne concernée, comme la minimisation des données, les technologies renforçant la protection de la vie privée; une plus grande transparence, un droit général et inconditionnel de s'opposer au traitement et la portabilité des données. »

[12] G29 - Avis sur la prise de décision individuelle automatisée et le profilage (2018, WP251rev.01), pages 20-21 :
"the Article 22(1) prohibition ***only*** *applies in specific circumstances when a decision based solely on automated processing, including profiling,* ***has a legal effect on or similarly significantly affects someone****, as explained further in the guidelines."*
"The GDPR does not define 'legal' or 'similarly significant' however the wording makes it clear that ***only serious impactful effects*** *will be covered by Article 22."*

[13] G29 - Avis sur la prise de décision individuelle automatisée et le profilage (2018, WP251rev.01), page 21 :
*"****A legal effect requires that the decision****, which is based on solely automated processing, affects someone's legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person's legal status or their rights under a contract."*

personnes concernées ; (ii) avoir un impact prolongé ou permanent sur la personne concernée; ou *(iii) dans sa forme la plus extrême, conduire à* ***l'exclusion ou à la discrimination*** *de personnes*[14]*. »*

Par ailleurs, le **CEPD** considère, dans ses lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux, **qu'aucune base légale n'est exclue par principe en matière de profilage**[15].

Ainsi, PERIFEM suggère des précisions de rédaction de l'exclusion proposée par la CNIL en matière de profilage, afin de reprendre les critères prévus à l'article 22 du RGPD (effets juridiques concernant la personne ou l'affectant de manière significative de façon similaire).

iii. Les émotions ne sont pas des données sensibles au sens du RGPD lorsqu'elles ne permettent pas d'identifier une personne de manière unique

Au §4.2.5.3, la CNIL propose d'interdire par principe la base de l'intérêt légitime pour les « *dispositifs qui analysent et segmentent les personnes sur la base de leurs émotions ou de données sensibles* », en mettant sur **le même plan ces deux catégories de données, sans distinction de la finalité des traitements.**

Pourtant, les émotions ne peuvent être qualifiées de données biométriques au sens du RGPD, et donc assimilées aux données sensibles, **qu'à condition de permettre ou confirmer l'identification unique d'une personne**[16]. Prenant ainsi l'exemple des photographies, le RGPD indique que « *le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que* ***celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique****.* »[17].

La CNIL a d'ailleurs précisé dans sa fiche sur la reconnaissance faciale que « *la technique biométrique de* ***reconnaissance automatisée*** *d'une personne, à partir des caractéristiques de son visage,* ***ne doit pas être confondue avec d'autres techniques de traitement des images (par exemple, avec des dispositifs de « vidéo intelligente » qui permettent de détecter des évènements ou des émotions sans reconnaître, pour autant, les individus****)* » [18].

Ainsi, PERIFEM propose des modifications de rédaction de l'exclusion proposée par la CNIL en matière d'analyse des émotions, afin de limiter l'exclusion aux dispositifs visant à identifier une personne de manière unique.

---

[14] G29 - Avis sur la prise de décision individuelle automatisée et le profilage (2018, WP251rev.01), page 21 :
« ***For data processing to significantly affect someone*** *the effects of the* ***processing must be sufficiently great or important to be worthy of attention****. In other words, the decision must have the* ***potential to:***
- *significantly affect the circumstances, behaviour or choices of the individuals concerned;*
- *have a prolonged or permanent impact on the data subject; or*
- *at its most extreme, lead to the exclusion or discrimination of individuals."*

[15] CEPD - Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux, Version 2.0 adoptées le 13 avril 2021 - §83 : « *Le ciblage des utilisateurs des médias sociaux à partir de données déduites à des fins publicitaires requiert généralement de réaliser un profilage. Le GT29 a précédemment clarifié que, selon le RGPD, le profilage se définit comme le traitement automatisé de données à caractère personnel consistant à évaluer certains aspects personnels, notamment pour analyser ou prédire des éléments concernant des personnes physiques, ajoutant que «[l]'utilisation du mot "évaluer" suggère que le profilage implique une certaine forme d'appréciation ou de jugement à l'égard d'une personne».* ***Le profilage peut être légal au regard de l'un quelconque des fondements juridiques de l'article 6, paragraphe 1, du RGPD, sous réserve de la validité de cette base juridique*** *»*

[16] RGPD - Article 4 : *«données biométriques, les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ; »*
RGPD - Article 9 : « *Le traitement des (…) données biométriques aux fins d'identifier une personne physique de manière unique, (…) sont interdits. »*

[17] RGPD - Considérant 51

[18] CNIL - Reconnaissance faciale : pour un débat à la hauteur des enjeux - 15 novembre 2019

iv. L'exclusion de l'analyse des comportements est antinomique avec le déploiement de la vision par ordinateur

Au §4.2.5.3, la CNIL propose enfin d'interdire par principe la base de l'intérêt légitime pour les « *dispositifs qui analysent le comportement et les émotions des personnes sur la base de la détection de leurs gestes et expressions, ou de leurs interactions avec un objet* », cette exclusion étant rédigée de manière particulièrement imprécise.

Si l'objectif de la CNIL est **d'exclure uniquement les dispositifs de reconnaissance biométrique,** et en particulier l'analyse des comportements à des fins d'identification unique[19], alors cet objectif est déjà atteint à travers le périmètre du projet de position qui écarte ce type de dispositifs (§1.3).

Si l'objectif de la CNIL est d'exclure les dispositifs qui analysent le comportement des personnes de manière générale et peu importe la finalité, alors cela pourrait aboutir à une interdiction générale des technologies de vidéo intelligente basées sur l'intérêt légitime. Or, cela ne semble pas être l'intention de la CNIL dans sa position, *a fortiori* puisqu'elle recommande une analyse des dispositifs au cas par cas (§2.2.7), et n'exclue aucune base légale par principe (§4.2.5.2).

Le **terme *« comportement »* recouvre des réalités d'usages diverses**, aux degrés d'implications variables sur les droits et libertés des individus. Par exemple, le comportement d'une personne peut être analysé pour détecter des chutes, à finalité de protection des personnes dans un espace public ; le comportement d'une personne peut aussi être analysé pour évaluer suivre son parcours en magasin et améliorer l'expérience client. **La balance des intérêts doit prendre en compte la finalité poursuivie, et non seulement les moyens mis en œuvre**.

Suggestion de rédaction du paragraphe 4.2.5.3

Option 1 : *suppression du paragraphe 4.2.5.3*

Option 2 : *nouvelle rédaction du paragraphe 4.2.5.3.*

La CNIL estime ainsi que ne pourraient en principe pas reposer sur l'intérêt légitime :

- *des dispositifs qui analysent et segmentent les personnes, sur la base de critères tels que l'âge ou le genre afin de leur adresser des publicités ciblées,* ***lorsque les décisions basées sur ces dispositifs produisent des effets juridiques concernant les personnes ou les affectent de manière significative de façon similaire, sens de l'article 22 du RGPD****;*
- *des dispositifs qui analysent et segmentent les personnes sur la base de leurs ~~émotions ou de~~ données sensibles (santé, religion, orientation sexuelle, etc.)* ***ou sur la base de leurs émotions lorsque celles-ci constituent des données biométriques au sens du RGPD****;*
- *des dispositifs qui analysent le comportement et les émotions des personnes sur la base de la détection de leurs gestes et expressions, ou de leurs interactions avec un objet,* ***lorsque les données analysées constituent des données biométriques au sens du RGPD ou lorsque les décisions basées sur ces dispositifs produisent des effets juridiques concernant les personnes ou les affectent de manière significative de façon similaire, sens de l'article 22 du RGPD****;*

[19] RGPD - article 4, alinéa 14 : *« données biométriques », les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou* ***comportementales*** *d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;*

2.3. COMMENTAIRES ET SUGGESTIONS SUR LA SECTION 4.3

- **<u>Une approche au cas par cas qui empêche une analyse générale du droit d'opposition</u>**

La position de la CNIL selon laquelle « *la plupart* » des dispositifs ne pourraient pas être mis en œuvre sans intervention législative et règlementaire apparaît contradictoire avec **l'appréciation au cas par cas** pourtant prônée par l'autorité (technologie aux multiples usages[20], pas le même degré d'intrusivité[21], marché très fragmenté[22] et hétérogène[23]).

En effet, la diversité d'usages implique *« des conditions de traitement **tout à fait variables**, et des **impacts différents sur la vie privée des personnes filmées.** »* (§2.2.5).

En cohérence avec l'approche casuistique par le risque proposée par la CNIL, PERIFEM recommande d'appliquer la même perspective s'agissant des conditions d'exercice du droit d'opposition.

- **<u>Une analyse du droit d'opposition partielle et non conforme aux recommandations européennes</u>**

Le droit d'opposition défini à l'article 21, alinéa 1er du RGPD[24] repose sur une série de conditions, dont la CNIL ne semble en retenir qu'une seule dans son projet de position, la temporalité de l'exercice de ce droit, et selon une interprétation partielle. Elle ajoute également à ce texte un critère qui n'y figure pas, la praticité de l'exercice du droit d'opposition, là encore selon une interprétation qui apparait incomplète.

PERIFEM souhaite exposer son analyse tant sur la temporalité (i) que sur la praticité du droit d'opposition (ii), et rappeler que le droit d'opposition comprend également d'autres conditions devant être prises en compte dans l'analyse au cas par cas des dispositifs (iii).

i. Le droit d'opposition peut être exercé avant ou pendant ou après le traitement

La CNIL part du principe que le droit d'opposition ne pourrait pas s'exercer avant ni pendant le traitement en matière de vidéos intelligentes, mais seulement après, ce qui rendrait ce droit ineffectif.

Pourtant, selon l'article 21 alinéa 1er du RGPD, « *La personne concernée a le droit de s'opposer à tout moment* », c'est-à-dire avant <u>ou</u> pendant <u>ou</u> après que le traitement ait été mis en œuvre.

C'est l'interprétation du Comité Européen pour la Protection des Données (« **CEPD** ») dans le contexte précis de la vidéoprotection :

[20] §2.2.7. *Dans ce contexte, une appréciation globale de ces dispositifs n'a pas de sens : il convient de les appréhender au cas par cas, en fonction en particulier des risques qu'ils comportent pour les intéressés.*
[21] §3.1.12. *Ces dispositifs, qui offrent un grand nombre d'usages et de fonctionnalités, ne présentent pas tous le même degré d'intrusivité.*
[22] §2.3.2. *Le marché de la vidéo « augmentée » est un marché mondial en croissance rapide, de quelque 7 % par an et estimé à 11 milliards de dollars en 202012, mais aussi très fragmenté.*
[23] §2.3.3 *Il s'agit d'un marché très hétérogène et très concurrentiel, avec des possibilités de croissance tant organique qu'externe.*
[24] RGPD - Article 21, alinéa 1er : « *La personne concernée **a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière,** à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.* »

« *Dans le contexte de la vidéosurveillance, la personne concernée peut formuler une objection* ***au moment d'entrer dans la zone surveillée, de traverser celle-ci ou après l'avoir quittée.*** *En pratique, cela signifie qu'à moins que le responsable du traitement ne puisse se prévaloir de motifs légitimes et impérieux, la surveillance d'une zone où il serait possible d'identifier des personnes physiques n'est licite que si :*

(1) le responsable du traitement est en mesure d'empêcher immédiatement la caméra de traiter des données à caractère personnel lorsque cela lui est demandé ; ***ou***
(2) la zone surveillée est délimitée de telle sorte que le responsable du traitement est certain d'obtenir l'accord de la personne concernée avant que celle-ci n'y pénètre et il ne s'agit pas d'une zone à laquelle la personne concernée a le droit d'accéder en temps normal.»[25]

Avant cela et dans le même sens, les lignes directrices du G29 concernant la prise de décision individuelle automatisée et le profilage soulignaient que : *«Une fois que la personne concernée exerce ce droit, le responsable du traitement doit* ***interrompre (ou éviter de démarrer)*** *le traitement à moins qu'il ne puisse démontrer des motifs légitimes et impérieux qui l'emportent sur les intérêts, les droits et libertés de la personne concernée. Le responsable du traitement peut également être amené à effacer les données personnelles données. »* [26]

Cette interprétation était d'ailleurs partagée par l'autorité de protection des données britannique lorsque le **Royaume-Uni** était soumis aux dispositions du RGPD[27], énonçant que l'exercice du droit d'opposition oblige le responsable de traitement **à stopper ou ne pas démarrer le traitement.**

De plus, l'affirmation de la CNIL « *En pratique, ces personnes pourront uniquement obtenir la suppression de leurs données, lorsqu'elles auront été conservées, et non éviter leur traitement. » (§4.3.3)* est inexacte. Par exemple, l'affichage d'un QR code à l'entrée d'un magasin permettant aux individus de scanner ce QR code pour désactiver le dispositif de vidéo intelligente avant même d'être entré dans son champ de vision constitue un exemple de droit d'opposition pouvant s'exercer en amont du traitement.

Cette position de la CNIL est d'ailleurs d'autant plus étonnante qu'en réalité, la majorité des traitements de données à caractère personnel classiques basés sur l'intérêt légitime ne permettent en pratique que l'exercice du droit d'opposition **après** le traitement. C'est par exemple le cas des traitements listés dans la fiche de la CNIL sur l'intérêt légitime[28].

PERIFEM propose donc à la CNIL d'assouplir son analyse de la temporalité du droit d'opposition, ainsi que cela figure dans sa suggestion de rédaction ci-dessous.

[25] CEPD - Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo - Adoptée le 29 janvier 2020: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf
[26] G29 - Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 - Version révisée et adoptée le 6 février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/wp251_profilage-fr.pdf
[27] ICO - Right to object : *Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals* ***to stop or prevent you from processing their personal data****.*
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/
[28] CNIL - L'intérêt légitime : comment fonder un traitement sur cette base légale ? https://www.cnil.fr/fr/les-bases-legales/interet-legitime : « *les traitements de données: visant à garantir la sécurité du réseau et des informations, mis en œuvre à des fins de prévention de la fraude, nécessaires aux opérations de prospection commerciale auprès de clients d'une société, portant sur des clients ou des employés au sein d'un groupe d'entreprises à des fins de gestion administrative interne ; prospection commerciale sur des produits analogues à ceux commandés par les clients d'une entreprise* ».

ii. Aucune modalité pratique du droit d'opposition n'est imposée par le législateur français et européen

La CNIL prétend que « *les conditions d'exercice du droit d'opposition apparaissent la plupart du temps, difficilement acceptables en pratique […] et feraient souvent peser une contrainte trop lourde ou irréaliste sur les individus* » (§**4.3.4**).

PERIFEM s'étonne de ce parti-pris et est convaincu que les technologies de vision par ordinateur offrent au contraire des **modalités de droit d'opposition simples et efficaces** pour les individus, en phase avec le RGPD qui encourage l'utilisation de **procédés automatisés** dans le cas de l'utilisation de services de la société de l'information[29].

Par exemple, **les *« QR codes »* à scanner** à l'entrée des magasins ou la mise en place de chemins alternatifs sont des modalités faciles, pratiques et non discriminatoires d'exercice du droit d'opposition.

***A contrario*, de nombreux traitements de données à caractère personnel plus classiques** ne mettant pas en œuvre de vidéos intelligentes et basés sur l'intérêt légitime, impliquent un exercice du **droit d'opposition beaucoup plus contraignant et moins efficace**. Dans sa fiche sur le droit d'opposition, la CNIL décrit l'exercice écrit du droit d'opposition, par voie électronique ou par courrier[30], qui implique : l'identification d'une adresse de contact du responsable de traitement, la rédaction d'un écrit, parfois la preuve de son identité et, enfin, le cas échéant, des échanges supplémentaires avec le responsable de traitement si celui-ci ne fait pas droit à la demande ou n'y répond pas dans le délai d'un mois.

PERIFEM présente ci-dessous une suggestion de rédaction alternative, afin de prendre en compte l'importance de modalités de droit d'opposition simples et efficaces.

iii. Les autres conditions de l'exercice du droit d'opposition

PERIFEM souhaite que la CNIL se positionne à la lumière de **l'ensemble des critères de validité du droit d'opposition, tels qu'énoncés par le RGPD**.

D'abord, contrairement aux autres droits dont disposent les personnes physiques en vertu du RGPD, **l'exercice du droit d'opposition requiert la démonstration de raisons tenant à la situation particulière de la personne concernée**. En ce sens, **le droit d'opposition est un droit relatif**, dont l'exercice doit être justifié auprès du responsable de traitement. Conformément au RGPD, la CNIL, dans sa fiche sur le droit d'opposition, souligne que le droit d'opposition permet de s'opposer à ce que des données soient utilisées par un organisme pour un objectif précis[31], dans la mesure où la personne apporte des **raisons suffisantes** à l'exercice de ce droit[32].

Ainsi, la CNIL a récemment rappelé que l'exercice du droit d'opposition *« **n'est pas automatique** : la personne qui l'exerce doit caractériser l'existence de raisons tenant à sa situation particulière. »* [33]. Dans le même sens, le Conseil d'Etat a refusé de valider une demande d'exercice de droit d'opposition dans la mesure où la requérante *« se bornait à invoquer des craintes d'ordre général concernant notamment la sécurité du*

[29] RGPD - Article 21(5)
[30] CNIL - https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees
[31] CNIL - https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees
[32] CJUE - affaire C-131/12 - Google Spain – Sous l'empire de la directive de 1995, le responsable de traitement devait déjà « examiner le bien-fondé » de la demande d'opposition - §71
[33] CNIL - Délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039468509

*fonctionnement de la base, **sans faire état de considérations qui lui seraient propres** ou seraient propres à ses enfants, pour en déduire qu'elle ne justifiait pas de motifs légitimes de nature à justifier cette opposition »* [34].

Or, dans le cadre d'une analyse au cas par cas, la CNIL pourra relever que, du fait de leurs modalités d'exercice, certains droits d'opposition mis en œuvre par des dispositifs de vidéo intelligente offrent une **garantie supplémentaire forte** pour les droits et libertés des individus, dans la mesure où ils permettent d'éviter le traitement de manière automatique, sans justification, offrant ainsi un **droit d'opposition inconditionnel**.

Le G29 considère à ce titre que : *« même si [ce droit] est subordonné à la présentation d'une justification par la personne concernée, **rien n'empêche le responsable du traitement de proposer une option de refus qui serait plus large**, et qui n'exigerait aucune démonstration supplémentaire d'un intérêt légitime (prépondérant ou autre) de la part de la personne concernée. Ce droit inconditionnel ne devrait pas se fonder sur la situation spécifique des personnes concernées. »*[35]

Ensuite, même si la personne concernée justifie de raisons tenant à sa situation particulière, le RGPD prévoit que le responsable de traitement peut en refuser l'exercice s'il démontre qu'il existe des ***« motifs légitimes et impérieux »*** pour le traitement qui **prévalent sur les intérêts et les droits et libertés de la personne concernée**, ou pour la constatation, l'exercice ou la défense de droits en justice. Le RGPD renverse ici la charge de la preuve[36] : le responsable de traitement devra donc, dans un second temps et au cas par cas, démontrer en quoi le refus d'exercice du droit d'opposition est **nécessaire à la préservation de ses intérêts**.

Le **CEPD** énonce dans les lignes directrices relatives au traitement des données à caractère personnel par des dispositifs vidéo[37] que *« **À moins que le responsable du traitement ne démontre que des motifs légitimes et impérieux** prévalent sur les droits et les intérêts de la personne concernée, le traitement des données de la personne qui s'est opposée doit alors cesser. ».*

Et il considère que la **sécurité des biens du responsable de traitement** peut fonder un motif légitime et impérieux : *« une entreprise rencontre des difficultés en raison de violations de la sécurité au niveau de son entrée publique et, s'appuyant sur l'existence d'un intérêt légitime, **utilise la vidéosurveillance afin d'identifier les personnes qui pénètrent illégalement dans ses locaux**. Un visiteur s'oppose au traitement de ses données par le système de vidéosurveillance pour des raisons tenant à sa situation particulière. Dans ce cas, l'entreprise rejette toutefois la demande en expliquant que **les images conservées sont nécessaires aux fins d'une enquête interne en cours et qu'elle a par conséquent des raisons légitimes et impérieuses de continuer à traiter les données à caractère personnel**. »* [38]

PERIFEM tient d'ailleurs à souligner que dans le cadre de traitements de données réalisés par des dispositifs de vidéo intelligente, **l'intérêt légitime d'une société privée peut converger avec un intérêt public**, notamment dans le cadre de dispositif de détection de mouvements suspects permettant d'améliorer la

[34] Conseil d'Etat - Décision du 18 mars 2019, 10ème - 9ème chambres réunies, 18/03/2019, affaire n°406313 https://www.legifrance.gouv.fr/ceta/id/CETATEXT000038244592/

[35] G29 - Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf

[36] CEPD - Lignes directrices 5/2019 sur les critères du droit à l'oubli au titre du RGPD dans le cadre des moteurs de recherche - Texte adopté le 7 juillet 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_fr.pdf

[37] CEPD - Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr

[38] CEPD - Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo - Adoptée le 29 janvier 2020 - §109 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr

protection des biens et des individus de manière individuelle et collective. Le G29 souligne[39] à ce titre que : ***« Plus l'intérêt public ou collectif est impérieux****, et plus la collectivité et les personnes concernées reconnaissent sans équivoque au responsable du traitement* ***la possibilité d'agir et de procéder au traitement de données pour servir ces intérêts et s'attendent à ce qu'il l'utilise, plus l'intérêt légitime pèse dans la balance****. »*

En ce sens, l'étude précitée réalisée par OPINION WAY et PERIFEM[40] démontre une **forte adhésion des Français à la vidéosurveillance** et à l'utilisation de caméras intelligentes. La position favorable exprimée par les individus concerne tout particulièrement des usages des caméras intelligentes destinés à **améliorer la sécurité dans les lieux publics, dont les commerces**, notamment la lutte contre les agressions ou le terrorisme, la lutte contre le vol en magasin, la propreté des espaces ou encore le respect de la règlementation liées aux incendies. **Cette forte adhésion est à prendre en compte dans la balance des intérêts.**

Enfin, **le responsable de traitement est en charge de déterminer la finalité** du traitement, d'effectuer une balance des intérêts en présence, et d'apprécier l'utilité du traitement mis en œuvre, et en particulier sa pertinence au regard du droit d'opposition proposé aux personnes concernées par rapport à la finalité poursuivie. Ainsi, dès lors que le traitement réalisé est licite et mis en œuvre de manière conforme à la règlementation applicable, le fait que les modalités du droit d'opposition fassent perdre de la qualité au traitement est un critère d'appréciation du seul ressort du responsable de traitement. Dans le cadre de traitements classiques mis en œuvre sur la base de l'intérêt légitime, tels que les traitements de données nécessaires aux opérations de prospection commerciale auprès de clients d'une société, le droit d'opposition constitue d'ailleurs toujours une limite pour le responsable de traitement, au bénéfice des personnes concernées. Le choix du responsable de traitement de mettre en œuvre le dispositif relève de sa liberté d'entreprendre, dès lors que la règlementation applicable est respectée.

PERIFEM propose donc une suggestion de rédaction ci-dessous, dans le but de prendre en compte l'ensemble des critères pertinents d'appréciation du droit d'opposition.

Suggestion de rédaction des paragraphes 4.3.1 à 4.3.7

4.3.1. À l'occasion de l'examen des différents cas d'usage portés à sa connaissance, la CNIL a estimé que ~~la plupart~~ ***certains*** *des dispositifs,* ***en particulier ceux mis en œuvre à des fins de police administrative ou judiciaire,*** *nécessitaient, pour pouvoir être légalement mis en œuvre, l'existence ou l'intervention d'un texte de nature législative ou réglementaire les autorisant et les encadrant.*

4.3.2. D'une part, la CNIL considère que les dispositifs de vidéo « augmentée » ~~se heurtent généralement en pratique à~~ ***doivent garantir, dans la plupart des cas d'usages, le respect de*** *l'obligation prévue par le RGPD de ~~garantir~~* ***donner*** *aux personnes concernées la possibilité de s'opposer au traitement de leurs données* ***pour des raisons tenant à leur situation particulière****.*

4.3.3. ***La conformité du droit d'opposition doit être appréciée au regard des critères imposés par le RGPD et la loi Informatique et Libertés.*** *Le droit d'opposition doit* ***d'abord*** *~~en effet~~ être garanti « à tout moment » par le responsable du traitement lorsque celui-ci se fonde sur un intérêt public ou son intérêt légitime.*

[39] G29 - Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE

[40] Etude OPINION WAY – PERIFEM « Les Français et la vidéosurveillance dans le commerce » - mars 2022 : **plus de 80% des Français accepteraient d'être filmés dans les magasins par des caméras intelligentes pour améliorer la sécurité des personnes et des biens**, et plus de 60% se déclarent favorables à ces technologies afin de faciliter leur expérience en magasin (propreté des espaces, fluidification du passage en caisse par exemple).

*~~Or,~~ **L**a mise en œuvre des dispositifs de vidéo « augmentée » dans l'espace public ou ouverts au public ~~apparait se heurter,~~ **doit respecter,** dans la pratique, l'obligation de prendre en compte et de respecter de manière effective ce droit d'opposition. ~~En effet, les~~ **Les** dispositifs vidéo **qui** captent automatiquement l'image des personnes passant dans leur spectre de balayage et la traitent souvent instantanément **doivent intégrer la possibilité pour les personnes d'exprimer leur droit d'opposition soit en empêchant le traitement, soit en interrompant celui-ci, soit en supprimant leurs données après le traitement.** ~~sans possibilité d'éviter les personnes ayant exprimé préalablement leur opposition ou d'interrompre le traitement. En pratique, ces personnes pourront uniquement obtenir la suppression de leurs données, lorsqu'elles auront été conservées, et non éviter leur traitement.~~ **La CNIL relève également que le responsable de traitement peut choisir de mettre en place un droit d'opposition inconditionnel, qui ne requiert pas une justification des personnes tenant à leur situation particulière. Ce choix permettant d'offrir une garantie supplémentaire pour les droits et libertés des individus, notamment en simplifiant et en automatisant les modalités d'exercice de ce droit. La CNIL rappelle enfin qu'il appartient au responsable de traitement qui ne fait pas droit à la demande d'opposition de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée. Ces intérêts peuvent résulter de l'existence d'un intérêt collectif coïncidant avec un intérêt privé du responsable de traitement, par exemple dans le cadre de dispositif mis en place pour la protection des biens et des individus.**

*4.3.4. La CNIL **invite les responsables de traitement, à la lumière des critères précités, à mettre en place des modalités d'exercice du droit d'opposition qui ne font pas peser de contrainte trop lourde ni irréaliste sur les personnes** ~~a pu constater que quelle que soit la bonne volonté des organismes à cet égard, les conditions d'exercice du droit d'opposition apparaissent la plupart du temps, difficilement acceptables en pratique, indépendamment de leur effectivité. Les modalités d'exercice envisageables font souvent peser une contrainte trop lourde, voire irréaliste, sur les personnes~~ (restriction importante de leurs possibilités de circulation, obligation d'adopter une gestuelle particulière ou de porter un signe distinctif stigmatisant...)**.** De plus, **la CNIL considère que les** modalités d'exercice du droit d'opposition ~~impliquent~~ **ne doivent pas impliquer** la mise en œuvre d'un traitement de données supplémentaire potentiellement plus intrusif (prise en considération de l'apparence vestimentaire des individus pour qu'ils soient reconnus lors de leur passage devant la caméra et automatiquement exclus du dispositif d'analyse des flux de fréquentation) **doivent être privilégiées par les responsables de traitement**. ~~Si l'on ne peut exclure que des développements techniques à venir permettent de mettre en place des modalités d'opposition équilibrée, la CNIL estime que tel n'est pas le cas actuellement.~~*

*4.3.5. Par ailleurs, l'existence même d'un droit d'opposition pourrait, dans certains, cas apparaître antinomique avec l'objectif poursuivi par le traitement : il en va ainsi de toutes les fois où il s'agit, pour des gestionnaires de lieux ouverts au public, de détecter des comportements anormaux, suspects ou dangereux à des fins de sécurisation des personnes et des biens. **Dans cette hypothèse, la CNIL invite les responsables de traitement à prendre en compte cette circonstance au stade de l'analyse d'impact afin de décider si le traitement conserve une légitimité et une utilité au vue de sa finalité.***

4.3.6 En conséquence, pour la CNIL, les dispositifs de vidéo « augmentée » devront, sous réserve de ne pas pouvoir justifier de la mise en œuvre effective et acceptable d'un droit d'opposition ou de pouvoir se prévaloir de l'exception liée à des traitements réalisés à des fins statistiques (cf. infra), être autorisés par un cadre légal spécifique de nature a minima réglementaire, conformément à l'article 23 du RGPD. Un tel acte devra acter la légitimité et la proportionnalité du traitement opéré au regard de l'objectif poursuivi, la nécessité d'exclure la faculté pour les personnes de s'y opposer, tout en fixant des garanties appropriées au bénéfice de ces dernières.

4.3.7. Cette analyse juridique rejoint la nécessité, pour la puissance publique, de tracer la ligne, au-delà du « techniquement faisable », entre ce qu'il est possible de faire, parce que socialement et éthiquement acceptable, et ce qu'il ne l'est pas. C'est un choix autant juridique, éthique que politique.

2.4. COMMENTAIRES ET SUGGESTIONS SUR LA SECTION 4.4

PERIFEM salue la prise de position de la CNIL sur les dispositifs de vidéo intelligente impliquant des traitements de données à des fins statistiques. Cette position constitue un pas de plus vers une **sécurité juridique accrue** pour les responsables de traitement, à travers une **clarification du cadre légal actuel**.

En effet, la France ayant opté pour l'exercice de la dérogation prévue à l'article 89.2 du RGPD[41], et ce à travers l'article 78 de la Loi Informatique et Libertés et le Décret °2019-536 du 29 mai 2019[42], les précisions et illustrations apportées par la CNIL sur le périmètre des dispositifs impliquant des traitements de données à des fins statistiques sont très utiles.

En particulier, PERIFEM relève que la CNIL va dans le même sens que le gouvernement (Premier ministre, Ministre délégué auprès de la ministre de la transition écologique, chargé des transports, Ministre de la transition écologique, Ministre des solidarités et de la santé) dans le Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports[43]. **La CNIL élargit son interprétation à d'autres cas d'usages, en particulier dans le cadre des magasins et centres commerciaux, et PERIFEM s'en félicite.**

PERIFEM entend apporter quelques précisions sur la notion de finalité statistique et son périmètre, et propose des légères modifications de rédaction de la position de la CNIL.

Depuis de nombreuses années, le Conseil de l'Europe considère que les traitements *« à des fins statistiques »* couvrent les opérations de traitement sur des données personnelles nécessaires pour des études statistiques et pour la production de résultats statistiques, et excluent tout usage des données obtenues **pour prendre**

---

[41] Article 89.2 du RGPD: *« Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, **le droit de l'Union** ou **le droit d'un État membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18 et 21**, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités. »*

[42] Article 116 du décret n° 2019-536 du 29 mai 2019 :

*Les dérogations prévues au deuxième alinéa de l'article 78 de la loi du 6 janvier 1978 susvisée relatif aux traitements à des fins de recherche scientifique ou historique ou à des fins statistiques s'appliquent uniquement dans les cas où les droits prévus aux articles 15, 16, 18 et 21 du règlement (UE) 2016/679 du 27 avril 2016 susvisé **risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités**.*

Les données issues de ces traitements conservées par le responsable du traitement ou son sous-traitant ne sont accessibles ou modifiables que par des personnes autorisées. Ces personnes respectent les règles de déontologie applicables à leurs secteurs d'activités. Les autorisations accordées par les responsables de traitement à ces personnes respectent les finalités spécifiques de l'alinéa précédent ainsi que les garanties prévues à l'alinéa suivant.

***Ces données ne peuvent pas être diffusées sans avoir été préalablement anonymisées sauf si l'intérêt des tiers à cette diffusion prévaut sur les intérêts ou les libertés et droits fondamentaux de la personne concernée. Pour les résultats de la recherche, cette diffusion doit être absolument nécessaire à sa présentation. Les données diffusées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées**. La diffusion de données à caractère personnel figurant dans des documents consultés en application de l'article L. 213-3 du code du patrimoine ne peut intervenir qu'après autorisation de l'administration des archives, après accord de l'autorité dont émanent les documents et avis du comité du secret statistique institué par l'article 6 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques en ce qui concerne les données couvertes par le secret en matière de statistiques.*

[43] Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports - https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043235679

des mesures ou des décisions concernant un individu en particulier[4445]. Ainsi, lorsque des informations sont utilisées à des fins statistiques, elles ne doivent être diffusées que de telle manière qu'il **soit impossible de les relier à une personne en particulier** et doivent ainsi être diffusées sous une forme agrégée[46].

Cette interprétation des données statistiques est reprise dans le **RGPD** au considérant 162[47], qui vise **deux critères cumulatifs** : (i) la production de **données agrégées**, et (ii) le résultat ne peut **impacter une personne physique en particulier**.

Au vu de ce qui précède, rien n'interdit l'usage des données statistiques (anonymisées et agrégées) dès leur production, à condition qu'elles n'impactent par une personne en particulier, mais un collectif de personnes. Par exemple, les cas d'usages des technologies de vidéos intelligentes aux fins de production de données statistiques relatives à la fréquentation d'un lieu sont importants pour permettre aux responsables de traitement d'utiliser ces technologies pour assurer la sécurité des personnes ou se conformer à des obligations légales (respect des jauges par exemple).

Suggestion de rédaction des paragraphes 4.4.3.1 et 4.4.3.2

4.4.3.1. Pour que ces traitements algorithmiques constituent un traitement de données à des fins statistiques, la CNIL considère qu'ils devront répondre aux conditions cumulatives suivantes :

- *En premier lieu, les résultats statistiques obtenus à partir du traitement de données ne doivent pas constituer des données à caractère personnel mais des données agrégées et anonymes au sens de la réglementation sur la protection des données.*
- *En second lieu, le traitement n'a une finalité statistique que s'il tend à la production de ces données agrégées pour elles-mêmes, afin de permettre éventuellement leur utilisation dans un second temps. Le fait, pour un dispositif qui se fonde sur une donnée agrégée, d'avoir une portée opérationnelle, pour permettre une réaction concrète en temps réel, **envers un individu particulier,** lui fait généralement perdre sa qualification de « statistique » et donc le bénéfice du régime dérogatoire afférent. En principe, la CNIL considère qu'il doit exister un délai entre la captation des données par le dispositif permettant la production des résultats statistiques et leur exploitation par le responsable du traitement.*

*4.4.3.2. Ceci joue de telle façon que, en cas d'utilisation de caméras augmentées pour calculer des statistiques sur un flux de personnes, l'éventuelle mesure prise par le responsable de traitement s'applique à un groupe de personnes **et non à des personnes en en particulier,** ~~nécessairement différent du groupe sur lequel porte l'information (la « statistique »). En outre~~, ainsi que le rappelle le considérant 162 du RGPD, les résultats statistiques ne sont en principe pas utilisés en tant que tels à l'appui d'une décision ou mesure concernant une personne physique en particulier*

[44] Conseil de l'Europe - Recommendation No R(97) 18, 30 septembre 1997, Page 2 *"Such operations exclude any use of the information obtained for decisions or measures concerning a particular individual"*

[45] Conseil de l'Europe - Resolution (74)29, Page 8 *« When information is used for statistical purposes it should be released only in such a way that it is impossible to link information to a particular person »*

[46] Conseil de l'Europe - Résolution (73)22 : *« Les données d'ordre statistique ne pourront être diffusées que sous une forme agrégée et de manière qu'il soit impossible de les attribuer à une personne déterminée. »*

[47] RGPD - Considérant 162 : *« Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais **des données agrégées, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier**. »*

Proposition de nouveau paragraphe après le 4.4.3.4 :

<u>À titre d'illustration additionnelle, la CNIL considère comme statistique un dispositif permettant le simple comptage de fréquentation d'un lieu public dans le but d'assurer la sécurité des personnes ou de se conformer à des obligations légales. Ce traitement, à partir de l'analyse des images issues des caméras présentes dans le lieu public, transmet uniquement des informations statistiques sur la fréquentation, à savoir le nombre de personnes présentes dans le lieu à un instant donné. Ce traitement sera considéré comme réalisé à des fins statistiques s'il n'a pas d'impact sur une personne en particulier mais la collectivité des personnes présentes dans le lieu, afin d'aider à réguler les flux entrant et sortant.</u>