Position ACN :

Position ACN sur la Consultation publique portant sur le Projet de Position de la CNIL relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics

11 mars 2022

INTRODUCTION

L'Alliance pour la Confiance Numérique (ACN) est l'organisation professionnelle qui représente les entreprises du secteur de la confiance numérique notamment celles des domaines de la cybersécurité, de l'identité numérique et de l'intelligence artificielle de confiance. Le monde de l'industrie de confiance numérique regroupe 2100 entreprises qui ont réalisé un chiffre d'affaires de 13,4 milliards d'euros en 2020. C'est un marché en forte croissance : plus de 8% par an en moyenne sur la période de 2016 à 2020. L'ACN rassemble plus de 90 entreprises représentant plus de 70% du chiffre d'affaires du secteur et qui sont à la fois des grands groupes leaders mondiaux, mais aussi 85% d'ETI, PME et start-up formant un écosystème extrêmement dynamique et innovant, notamment dans le domaine de l'IA de confiance.

La CNIL a rendu public et a mis en consultation publique son Projet de Position relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics.

L'ACN se réjouit de cette démarche d'association des acteurs économiques privés concernés par ce sujet ainsi que de l'ambition affichée par la CNIL de clarifier les notions utiles à la bonne appréhension des enjeux liés à l'utilisation des systèmes d'intelligence artificielle sur des dispositifs vidéo, et sa soumission à une consultation publique.

L'ACN entend, à travers la réponse à cette consultation, formuler des commentaires relatifs au projet de position de la CNIL autour des axes suivants :

- **L'intelligence artificielle de confiance est une technologie aux multiples usages créatrice de valeur et vecteur de création et de transformation d'emplois. Un tissu français d'entreprises de toutes tailles, extrêmement diverses, constitue un écosystème particulièrement riche, innovant et dynamique dans ce domaine.**
- **Dans le domaine de l'intelligence artificielle, l'ACN considère qu'un raisonnement fondé sur la technologie *per se* n'est pas opportun et ne répond pas aux défis sociétaux posés par les évolutions des technologies.**

- **L'ACN recommande, en conséquence, d'adopter une vision différenciée, par usages ou familles d'usages permettant d'appréhender les risques au cas par cas ainsi que les moyens à mettre en œuvre pour assurer une protection optimale des données personnelles ainsi que des libertés et droits fondamentaux des citoyens.**

- **Les clients utilisateurs de ces technologies ainsi que les entreprises du secteur doivent être aidés dans leur démarche de mise en œuvre de leurs technologies dans le plein respect des libertés et droits fondamentaux :**

    - **L'encadrement et les définitions des usages et des risques qui leur sont associés doivent s'appuyer sur des référentiels clairs, objectifs et reflétant l'état de l'art.**

    - **Les moyens pour une entreprise de démontrer le caractère respectueux d'une solution au regard des impératifs précités doivent être définis, par exemple sous forme de certification. Celle-ci doit permettre de distinguer les solutions et doit viser à conférer un avantage compétitif aux acteurs s'étant engagés dans cette voie.**

    - **Le recours à des jeux de données est indispensable à l'innovation à l'entrainement et au développement des technologies d'IA : il est vital pour les entreprises du secteur d'avoir accès à des jeux de données présentant les garanties jugées nécessaires au regard notamment de la problématique des biais, ou de disposer de règles précises permettant de constituer puis d'utiliser des tels jeux de données à des fins d'entrainement et de développement uniquement.**

En conclusion, l'ACN se félicite que la CNIL reconnaisse parmi ses objectifs celui de faire émerger des fleurons français de l'IA. En effet, ces technologies sont indispensables à la maîtrise de notre avenir et de notre souveraineté numérique. Il est donc indispensable de mener une réflexion de fond pour qu'une vision indiscriminée de la défense des droits et libertés fondamentaux n'ait pas comme résultat d'annihiler toute innovation et développement des acteurs européens. Si les seuls outils et technologies disponibles sont conçus, développés et maitrisés dans d'autres systèmes de valeur dont la compatibilité avec les droits et libertés fondamentaux européens doit être questionnée, alors l'objectif de protection des droits et libertés fondamentaux serait ainsi impossible à atteindre. L'ACN relève également la volonté de dialogue et de dynamisme de la CNIL à travers les différents échanges qui ont été réalisés et qui ont permis l'émergence d'un canal de confiance avec les industriels.

1. Commentaires et suggestions sur la Partie 2 – La vidéo augmentée : portrait d'une technologie aux multiples usages.

L'ACN partage le constat qu'une « *appréciation globale de ces dispositifs n'a pas de sens* » et qu'une appréhension « *[…] au cas par cas, en fonction en particulier des risques […]* » (§2.2.7) semble être la bonne solution ; toutefois, à la vue du grand nombre d'utilisations envisageables, il semblerait opportun de **détourer des familles d'usages permettant d'aider au positionnement des différentes technologies** (une proposition s'articulant autour de la distinction des usages à finalité statistique et opérationnelle pourrait être une première étape).

L'ACN voudrait rappeler que le traitement de données opéré par les algorithmes de traitement d'images ne donne pas lieu à « *changer la nature et la portée de la vidéo* » (§2.1.4), mais change uniquement la nature de l'usage qui en est fait, en multipliant les capacités des dispositifs vidéo.
Et contrairement à ce qui est affirmé, « *la principale motivation du déploiement des dispositifs de vidéo augmentée* » n'est pas « *le gain en termes de coût permis par la réduction des effectif*s » (§2.3.6), mais l'apport une valeur ajoutée aux tâches de chacun. L'ACN souhaiterait que la CNIL puisse préciser sur quel texte de référence elle fonde son affirmation.
Pour illustrer nos propos, la technologie permettant d'aider à la détection des vols à l'étalage n'a pas vocation à supprimer des emplois, mais à améliorer l'efficacité et le travail des agents de sécurité, en leur indiquant où et quand regarder en temps réel sur leurs écrans grâce à des gestes objectifs de vol. Le principal utilisateur de cette technologie est l'agent de sécurité. Un groupe qui déploie cette solution à grande échelle a par exemple recruté 20 postes à temps plein d'agents de sécurité supplémentaires pour utiliser et exploiter leur solution sur l'année 2021. Il est important de mettre en exergue l'apport en productivité permis par cette technologie qui crée plus de valeur sans nécessairement imposer de monter en compétence. **L'ACN appuie sur le fait que l'intelligence artificielle de confiance n'a non pas pour vocation de supprimer de l'emploi mais d'en créer, et de créer de la valeur pour tous les acteurs en délestant les opérateurs des tâches ancillaires pour leur permettre de se concentrer sur les tâches les plus pertinentes. Cette technologie est un accompagnement dans la transformation des métiers.**

De plus, il semble étonnant dans le cadre des usages de cette technologie pour des missions de police administrative et judiciaire d'énoncer que la détection automatisée de situation permettrait de « *[…] présumer la commission d'infractions* » (§2.2.3).
L'ACN tient à mentionner que dans le cadre des usages multiples de l'IA, cette technologie peut aider à la détection de situations pouvant conduire à une infraction, mais ne prend pas, à date, de décision finale automatisée. **C'est une simple aide à la décision qui laisse la liberté à l'homme de contrôler/confirmer/infirmer. En aucun cas, l'algorithme ne**

peut « *présumer* » de la commission d'une infraction au sens juridique du terme. Il semblerait opportun de clarifier l'utilisation de ce terme.

Synthèse :

1. Il est indispensable de détourer des familles d'usages permettant d'appréhender les technologies au cas par cas et d'être éclairé sur le régime juridique applicable.
2. L'intelligence artificielle est une aide à la détection et à la décision, cette technologie ne prend pas, à date, de décision automatisée issue d'une présomption de commission à une infraction.
3. Il faut appuyer sur le fait que l'intelligence artificielle de confiance n'a pas pour objet de supprimer de l'emploi, mais d'accompagner la transformation des métiers et d'en créer de nouveaux.

2. Commentaires et suggestions sur la Partie 3 – Une technologie porteuse de risques gradués pour les droits et libertés des personnes.

Dans cette section spécifique aux risques particuliers apportés par cette technologie aux droits et libertés des personnes, il semble important de rappeler que cette consultation et ce projet de position doivent participer à favoriser l'émergence de leaders français de l'intelligence artificielle de confiance et non pas aboutir à des règles ou des situations qui pourraient entraver leurs développements à la faveur d'acteurs non souverains. A l'heure où les entreprises non européennes ont des facilités de développement du fait de cadres juridiques plus larges, notamment sur la création et l'utilisation de jeux de données pour l'entraînement des IA, des enjeux de compétition internationale et de concurrence doivent pousser les instances à édicter des règles favorisant les leaders souverains et européens.

Les règles édictées ne doivent pas porter uniquement sur les usages de cette technologie, mais également encadrer de manière équitable tous les acteurs de la chaine (fabricants d'équipements, fabricants de logiciels, intégrateurs, opérateurs de service, clients finaux…). Les contraintes liées au développement des solutions doivent être similaires pour tous et suivre les directives et les orientations de la Commission européenne (respect des libertés et droits fondamentaux, obligation de transparence, absence de discrimination …).

L'ACN voudrait revenir sur l'utilisation de termes appelant à questionnement. Dans son projet de position, la CNIL parle d'un « *potentiel de versatilité* » que présentent les technologies de vidéo augmentées (§3.1.10). Or, l'utilisation du terme « versatilité », défini dans le Larousse comme « *qui change facilement d'opinion, qui est sujet à des voltes-faces subites* », a une connotation négative et anxiogène, ce qui porte à questionnement sur le sens recherché. L'utilisation d'une intelligence artificielle appelle à la confiance dans les

algorithmes et dans les entreprises qui les développent et les mettent en œuvre ; ces derniers sont configurables et déterministes et non pas versatiles. S'il faut entendre « détournement de finalité » comme énoncé précédemment par la CNIL, il faut préciser les nuances apportées par ce changement de terminaison.

De plus, pour permettre que ces dispositifs de traitement algorithmique soient de confiance, et limitent « *les erreurs et les biais qui pourraient avoir un impact important sur les personnes* » (§3.1.11) au maximum, il existe des solutions. Il faudrait **constituer des jeux de données vidéo, contenant des données à caractère personnel, prises dans l'espace public, ce qui n'est pas envisagé dans le RGPD ou le projet d'IA Act, mais qui est nécessaire pour permettre l'entrainement et ainsi développer une IA européenne performante et compétitive.**
De plus, pour évaluer correctement ces jeux de données et ainsi aller jusqu'au développement d'une IA de confiance en évitant les biais, il faut permettre l'évaluation de ces jeux de données par des critères prédéfinis et communiqués ou par la construction de certifications.

La CNIL parle également *« d'informations en sommeil »* (§3.1.2). L'utilisation de ces termes appelle également à questionnement. L'ACN souhaiterait que soit affinée et expliquée cette terminologie afin de pouvoir tirer les conséquences juridiques du traitement de ces données.

L'ACN relève la justesse de la conclusion de la CNIL énonçant que « *ces dispositifs, offrent un grand nombre d'usages et de fonctionnalités* » et « *ne présentent pas tous le même degré d'intrusivité* » (§3.1.12). Toutefois, **il semblerait opportun de construire avec le soutien des industriels un « guide/tableau » permettant de classer par famille de cas d'usage les degrés d'intrusivité afférents.**
L'approche par risques graduée utilisée par la CNIL semble être la bonne, comme l'a déjà relevé l'ACN ; toutefois, dans le cadre des échantillons retenus pour l'analyse vidéo (§3.2.2 et §3.2.3), la CNIL ne doit pas confondre le nombre de sujets sur lequel porte l'analyse et la finalité de la décision. **Le risque sur les libertés fondamentales des sujets doit être mis en balance avec la finalité collective ou individuelle de la décision et non pas avec le nombre de personnes touchées par l'analyse**.

La CNIL énonce que l'impact de ces dispositifs alors même qu'ils ont une finalité collective pourrait varier en fonction des lieux de déploiement et des populations les fréquentant. Pour illustrer ses propos, elle utilise les centres commerciaux ou les magasins de jeux vidéo comme « *[…] par nature, […] souvent fréquentés par des mineurs* » (§3.2.5) et donc nécessitant une attention particulière. L'ACN voudrait avoir des explications concernant ce constat et la source de cette affirmation.

Synthèse :

1. La constitution de jeux de données vidéo, contenant des données à caractère personnel, prises dans l'espace public est nécessaire pour permettre l'entrainement et le développement de l'IA. De plus, une évaluation de ces jeux de données selon des critères prédéfinis/certifications permettrait d'éviter les biais et de construire une IA de confiance.
2. Pour permettre aux entreprises de connaitre le régime applicable et les risques liés à leurs technologies, la CNIL pourrait, avec l'aide des industriels, établir un classement des degrés d'intrusivité afférents aux familles de cas d'usage.
3. L'approche par risque graduée est la bonne, toutefois, les risques sur les droits et libertés fondamentaux des sujets doivent être mis en balance avec la finalité collective ou individuelle de la décision, et non pas avec le nombre de personnes touchées par l'analyse.
4. L'utilisation de termes laissant sous-entendre des aspects négatifs intrinsèques à la technologie ne semble pas être une approche favorable à l'émergence d'une IA souveraine et européenne de confiance.

3. Commentaires et suggestions sur la Partie 4 – Des conditions de légalité différenciées en fonction des objectifs, des conditions de mise en œuvre et des risques de dispositifs de vidéo « augmentée ».

De nombreux textes juridiques sont mobilisés dans l'utilisation de l'intelligence artificielle (Loi Informatique et Liberté – LIL, RGPD). Les IA de traitement de l'image sont des logiciels qui viennent en surcouche par rapport à des solutions indépendantes (vidéoprotection ou simple caméra), se traduisant juridiquement par un nouveau traitement rendant l'imbrication des différents textes déjà existants complexe.
L'ACN salue les clarifications de la CNIL sur le champ d'application du Code de la Sécurité Intérieure (CSI) qui ne vient pas « *[…] spécifiquement encadrer les conditions de mise en œuvre des dispositifs de vidéo augmentée* » (§4.1.3), mais voudrait que **la CNIL à travers son analyse à droit constant fasse un effort de pédagogie pour permettre au client final d'avoir une meilleure compréhension du cadre juridique sur lequel s'appuyer pour déployer sa solution. Un éclaircissement juridique permettrait de lever un frein entravant le développement des projets et causant un impact économique lourd sur les entreprises créatrices d'IA de confiance.**
L'articulation juridique du CSI, du RGPD et de la LIL crée aujourd'hui une confusion pour les responsables de traitement. En effet, les algorithmes viennent souvent en support pour les équipes opérationnelles dans le cadre de leurs missions premières encadrées par le CSI et deviennent donc une « extension » des outils déjà utilisés. Il pourrait être souhaitable que l'intelligence artificielle soit intégrée au CSI pour les finalités liées à la vidéoprotection.

Pour ce qui est de la base légale appropriée, la CNIL relève que « *[…] certains dispositifs ne pourront en principe pas se fonder sur l'intérêt légitime […]* » (§4.2.5.2), elle cite trois exclusions sans les expliciter (§4.2.5.3[1]). **Il semble important que la CNIL justifie et clarifie ce qu'elle entend par ces exclusions et leur cadre légal applicable**.
La CNIL n'exclut pas les dispositifs d'analyse du comportement des personnes de manière générale, et laisse entendre une utilisation possible de cette technologie dans un cadre de nécessité et de proportionnalité du dispositif. En parlant de « *[…] responsable du traitement devant justifier de la nécessité d'utiliser des systèmes de vidéo « augmentée »* (§4.2.6.1), la CNIL laisse la possibilité d'utiliser cette technologie, mais impose une « *évaluation* » de nécessité sans préciser quels seraient les résultats attendus pour mettre en place cette technologie. **L'ACN souscrit à une utilisation nécessaire et proportionnée de la technologie, mais souhaite que les critères d'évaluation soient prédéfinis et communiqués afin de pouvoir développer des solutions optimales qui seront compatibles et qui permettront d'arriver aux résultats attendus.**
L'ACN soulève les recommandations posées par la CNIL en matière de « *[…] mécanismes effectifs de protection de la vie privée* » (§4.2.6.2) notamment à travers le *privacy by design,* floutage et traitement local des données. Toutefois, l'ACN souhaiterait que la CNIL apporte plus de détails sur la distinction des effets entre un dispositif physiquement accolé aux caméras et un système de traitement centralisé.

En affirmant la nécessité de normes autorisant et encadrant la plupart des dispositifs pour permettre leur mise en œuvre, la position de la CNIL apparait contradictoire avec l'appréciation au cas par cas prônée dans le projet de position.
Elle énonce notamment que certains dispositifs de vidéo augmentée, dont ceux mis en œuvre pour aider à la décision dans le cadre de prérogatives de police administrative ou judiciaire, sont particulièrement « *[…] susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques* » (§4.3.8).
Cependant, il est possible de nuancer cette affirmation ; l'ACN peut proposer une **liste d'infractions fondée sur celles de la vidéo verbalisation dans laquelle la technologie ne modifie en rien la nature de l'infraction, mais est une réelle aide dans la décision d'intervention :**

- Le non-respect des signalisations imposant l'arrêt des véhicules (feu rouge, stop…) ;
- Le non-respect des vitesses maximales autorisées ;
- Le non-respect des distances de sécurité entre les véhicules ;
- L'usage de voies et chaussées réservées à certaines catégories de véhicules comme les bus et les taxis ;

[1] 1- 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 ;
2- Des dispositifs qui analysent et segmentent les personnes sur la base de leurs émotions ou de données sensibles (santé, religion, orientation sexuelle, etc.) ;
3- 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.

- Le défaut du port de la ceinture de sécurité ;
- L'usage du téléphone portable tenu en main ;
- La circulation, l'arrêt, et le stationnement sur les bandes d'arrêt d'urgence ;
- Le chevauchement et le franchissement des lignes continues ;
- Le non-respect des règles de dépassement ;
- Le non-respect des sas vélos ;
- Le défaut de port du casque à deux-roues motorisé ;
- Les véhicules en contre-sens ;
- Le stationnement gênant, dangereux, interdit ;
- Les Dépôts Sauvages ;
- La circulation véhicules interdits dans certaines voies/espaces et par catégorie de véhicules.

Dans le cadre de ces infractions, l'impact de la technologie pour la personne est moindre.

L'ACN a également des commentaires et suggestions à faire sur le droit d'opposition dans le cadre du déploiement de dispositifs de vidéo « augmentée » (Section 4.3).

L'approche au cas par cas retenue par la CNIL dans son projet de position semble incompatible avec une analyse générale du droit d'opposition. En effet, la diversité des usages implique nécessairement « *des conditions de traitement tout à fait variables, et des impacts différents sur la vie privée des personnes filmées* » (§2.2.5) ; il semblerait donc logique d'apposer cette même logique s'agissant des conditions d'exercice du droit d'opposition.

De plus, le Comité Européen de Protection des Données (CEPD) reconnait, dans ses lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo[2], la spécification du traitement vidéo et la difficulté technique d'appliquer le droit d'opposition avant de pénétrer dans un site équipé d'une solution d'analyse vidéo qui couvrirait ses entrées. Il appelle notamment à pouvoir pratiquer ce droit au moment où a lieu l'entrée sur le site et non avant (considérant 106 des lignes directrices[3]). La mise en place d'un droit d'opposition semble donc possible ; il est envisageable d'imaginer la mise en place d'un bouton poussoir à l'entrée d'un espace pouvant accueillir le public dont la pression entrainerait l'arrêt total du traitement pour une durée déterminée.

D'autre part, le caractère relatif du droit d'opposition est rappelé dans le RGPD « *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 […]. Le responsable de traitement ne traite plus les données à caractère personnel, à moins qu'il*

[2] 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

[3] Ibid, considérant 106 « 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. »

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 » (Chapitre 3, Section 4, Article 21 – Droit d'opposition)[4]. Le CEPD appuie également sur la relativité de ce droit, dans ses lignes directrices, en ce qui concerne « *la vidéo surveillance fondée sur un intérêt légitime ou la nécessité d'exécuter une mission d'intérêt public la personne concernée a le droit de s'opposer, à tout moment […] au traitement conformément à l'article 21 du RGPD. A moins que le responsable de traitement ne démontre que les motifs légitimes et impérieux prévalent sur les droits et intérêts de la personne concernée, le traitement des données de la personne qui s'est opposée doit alors cesser* »[5].

L'ACN voudrait également souligner la pertinence du raisonnement de la CNIL relatif au « *cas spécifique des dispositifs impliquant des traitements de données à des fins statistiques* » (Section 4.4) dans lequel elle énonce « *qu'un certain nombre de dispositifs de vidéo « augmentée » […] destinés à réaliser des comptages conduisant à des analyses statistiques* » (§4.4.1) peuvent répondre à des critères « *permettant l'application d'un régime dérogatoire au titre duquel il est notamment permis d'exclure, le cas échéant, le droit d'opposition des personnes concernées* »[6] (§4.4.2).

L'ACN voudrait mettre en avant le fait qu'au vu des multiples usages possibles des dispositifs de vidéo augmentée, l'exercice du droit d'opposition n'est pas impossible par nature. L'ACN propose donc à la CNIL d'assouplir son analyse afin de prendre en compte des modalités d'adaptation simples et efficaces du droit d'opposition et ainsi travailler vers une posture en fonction des usages.

Synthèse :

1. Il serait souhaitable que la CNIL fasse preuve de pédagogie et précise les imbrications des différents textes applicables aux technologies d'intelligence artificielle pour permettre au client final de clarifier les fondements juridiques sur lesquels s'appuyer pour déployer la solution.
2. En excluant le fondement de l'intérêt légitime dans trois cas de figure non explicités, le projet de position peut aboutir à une interdiction globale des technologies de vidéo intelligente fondées sur le comportement des personnes de manière générale, peu importe leur finalité. C'est pourquoi il est important que la CNIL justifie et clarifie ce qu'elle entend par ces exclusions et leurs implications.
3. L'ACN souscrit à une évaluation de la nécessité et de la proportionnalité de la technologie, mais souhaite que les critères d'évaluation soient prédéfinis et communiqués afin de pouvoir développer des solutions optimales et compatibles permettant d'arriver aux résultats attendus.

[4] RGPD, Chapitre 3 – droits de la personne concernée : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3
[5] Op cit – CEPD lignes directrices, considérant 105.
[6] Article 89 du RGPD éclairé par son considérant 162, article 78 de la Loi Informatique et Libertés et 116 de son décret d'application (décret n°2019-536 du 29 mai 2019).

4. L'ACN voudrait mettre en avant le fait qu'au vu des multiples usages possibles des dispositifs de vidéo augmentée, l'exercice du droit d'opposition n'est pas impossible par nature. Et propose donc à la CNIL d'assouplir son analyse afin de prendre en compte des modalités simples et efficaces du droit d'opposition et ainsi travailler vers une posture d'atténuation de ce droit d'opposition relatif en fonction des usages.
5. La technologie ne modifie pas nécessairement la nature de l'infraction incriminée, l'ACN propose une liste d'infractions fondées sur la vidéo verbalisation dans laquelle la technologie ne modifie en rien la nature de l'infraction.