



Décision MED-2024-150 du 15 novembre 2024

Commission Nationale de l'Informatique et des Libertés

Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 05 décembre 2024

Décision n° MED-2024-150 du 15 novembre 2024 mettant en demeure le ministère de l'intérieur

(N° MDM 241080)

Conformément à la décision n° 2023-259C du 15 novembre 2023, la Commission nationale de l'informatique et des libertés (CNIL) a effectué un contrôle sur pièces du ministère de l'Intérieur et des Outre-mer (ci-après, le " ministère de l'Intérieur ") le 6 décembre 2023 ainsi que des contrôles sur place auprès des direction de la police judiciaire de la préfecture de police de Paris (DPJ-PP) et service central de renseignement criminel de la gendarmerie nationale (SCRC-GN). [...]

Cette procédure de contrôle avait pour objet d'apprécier la conformité des traitements de données à caractère personnel relatifs aux logiciels de traitements d'analyse automatisée des images (ci-après, " logiciels d'analyse vidéo ") mis en œuvre par le ministère de l'Intérieur ou pour son compte aux dispositions de la loi n° 78-17 du 6 janvier 1978 (la loi " Informatique et Libertés "), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (le " RGPD "), de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 (la directive " Police-Justice ") ainsi que des dispositions prévues aux articles L. 233-1 et suivants et L. 251-1 et suivants du code de la sécurité intérieure (CSI).

À titre liminaire, je vous rappelle que cette décision de contrôle a été prise suite à la publication par le journal d'investigation *Disclose*, le 14 novembre 2023, d'une enquête révélant l'utilisation par les services du ministère de l'Intérieur d'un logiciel d'analyse vidéo commercialisé par la société BRIEFCAM. Cette enquête indiquait que plusieurs directions et services du ministère, commissariats de police et brigades de gendarmerie auraient utilisé, progressivement depuis 2015, ce logiciel afin notamment de rechercher un individu en fonction de différents critères. Selon cette enquête, ce logiciel disposerait également d'une fonctionnalité de reconnaissance faciale, laquelle serait utilisée par différents services du ministère.

Concomitamment à l'ouverture par la CNIL de cette procédure de contrôle, le ministre de l'Intérieur et des Outre-mer a annoncé le 17 novembre 2023 " *une mission inter-inspections sur l'utilisation de logiciels d'analyse vidéo par les services de police et gendarmerie nationales* ".

Dans le cadre de la procédure de contrôle de la CNIL, une réponse au questionnaire adressé au ministère de l'Intérieur, le 6 décembre 2023, a été apportée à la Commission le 18 mars 2024.

Suite à ces premiers éléments de réponse, des contrôles sur place ont eu lieu auprès de la DPJ-PP le 15 mai 2024 et du SCRC-GN le 21 mai 2024.

Les constatations effectuées lors de ces contrôles me conduisent à relever les éléments suivants.

I- Analyse des faits en cause

1. Sur le manquement à l'obligation de traiter des données de façon licite

En droit, d'une part, l'article 4, 1°, de la loi " Informatique et Libertés " dispose que les données à caractère personnel doivent être " *traitées de manière licite, loyale* ".

Par ailleurs, **l'article 87 de cette loi** prévoit que les traitements de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales " *ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission*

effectuée, pour l'une des finalités énoncées au premier alinéa, par une autorité compétente au sens du même premier alinéa et où sont respectées les dispositions des articles 89 et 90".

L'article 89 de cette loi précise quant à lui que " si le traitement est mis en œuvre pour le compte de l'État pour au moins l'une des finalités énoncées au premier alinéa de l'article 87, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au I de l'article 31 et aux articles 33 à 36 ". Ces derniers articles prévoient que les traitements doivent être autorisés, selon les cas par arrêté ou décret et que, lorsqu'un acte réglementaire unique autorise un ensemble de traitements similaires, chaque traitement doit ensuite faire l'objet d'une déclaration à la CNIL prenant la forme d'un " engagement de conformité ".

D'autre part, l'exploitation des enregistrements visant à identifier *a posteriori*^[1] les auteurs présumés d'infractions constitue une technique d'investigation encadrée par le code de procédure pénale (CPP)^[2]. Les dispositions précitées des articles 87 et 89 de la loi " Informatique et Libertés " sont applicables à ces traitements.

À cet égard, la CNIL considère que l'exploitation d'enregistrements vidéo par le biais d'un logiciel d'analyse vidéo peut être autorisée, notamment si ce dernier constitue un **logiciel de rapprochement judiciaire** (ci-après, " LRJ ").

Afin d'être utilisé de façon licite, un logiciel d'analyse vidéo utilisé comme logiciel de rapprochement judiciaire doit être mis en œuvre dans le cadre défini au sein des CPP^[3] et décret n° 2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle (ci-après, le " décret du 7 mai 2012 "). En particulier, ce décret impose que la mise en œuvre de tels logiciels soit précédée d'un engagement de conformité, accompagné d'une AIPD^[4], adressé à la CNIL^[5] – permettant à cette dernière d'exercer ses pouvoirs de contrôles^[6] (v. *infra*).

À cet égard, la Commission a précisé dans son avis rendu en séance plénière le 15 décembre 2011 concernant le projet de ce décret que " la mise en œuvre de chaque [LRJ] utilisé par la police nationale, la gendarmerie nationale ou la préfecture de police, devra ainsi être précédée de l'envoi d'un engagement de conformité faisant référence au [dit] décret ". Dans cet avis, la Commission a également précisé que " d'autres logiciels [que les logiciels ANACRIM-ATRT et ANACRIM-ANB] mis en œuvre par la gendarmerie nationale, la police nationale et la préfecture de police, devraient par la suite être présentés à la Commission "^[7]. Par cet engagement adressé à la CNIL, l'organisme déclarant atteste de la conformité de son traitement de données à caractère personnel à l'acte réglementaire unique " RU-018 – Logiciel de rapprochement judiciaire à des fins d'analyse criminelle " (ci-après, " RU-018 ")^[8], à l'appui d'un dossier technique de présentation du logiciel en question.

Enfin, je relève que le cadre juridique des LRJ prévoit des garanties fortes pour les droits et libertés des personnes. Ce type de logiciels, qui doit nécessairement s'inscrire dans le cadre d'une enquête judiciaire^[9], ne peut en particulier être mis en œuvre que sous le contrôle, notamment, du magistrat saisi de l'enquête ou chargé de l'instruction^[10].

En l'espèce, dans la réponse au contrôle sur pièces précité que vos services ont adressée aux miens le 18 mars 2024, ainsi qu'au cours des contrôles sur place effectués auprès des DPJ-PP et SCRC-GN en mai dernier, il a été indiqué que le ministère de l'Intérieur utilise des logiciels d'analyse vidéo depuis l'année 2015.

Lors du contrôle effectué auprès du SCRC-GN, il a été indiqué à la délégation que " L'édiction d'un décret ad hoc, spécifiquement dédié aux logiciels d'analyse vidéo, a initialement été envisagée par la direction générale de la Police nationale (DGPN). Après analyse, la DLPJ a considéré en janvier 2023 que les logiciels d'analyse vidéo relevaient de l'actuel cadre relatif aux logiciels de rapprochement judiciaire (LRJ). ". Il a également été précisé à la délégation de contrôle que " Lors de l'utilisation du logiciel de la société BRIEFCAM à compter de 2018, le SCRC considérait ce logiciel comme un nouvel outil d'analyse vidéo "^[11].

Or, en premier lieu, s'agissant de la direction générale de la Gendarmerie nationale (DGGN), je relève que le logiciel souverain " Système V " (ex- " Sigma enquêteurs ")^[12] est notamment utilisé depuis 2021. Or, je relève que la DGGN a transmis à la CNIL un engagement de conformité au RU-18 concernant la mise en œuvre de ce logiciel le 20 novembre 2023, soit deux ans après le début de son utilisation.^[13] Par ailleurs, s'agissant du SCRC-GN, je relève que, malgré l'utilisation depuis 2018 du logiciel d'analyse vidéo édité par la société BRIEFCAM, l'engagement de conformité n'a été transmis à la CNIL que le 7 octobre dernier, soit cinq ans après le début de son utilisation.

En deuxième lieu, s'agissant de la DGPN, je relève que, malgré l'utilisation depuis 2015 de plusieurs logiciels édités par la société BRIEFCAM par certains services de la direction, l'engagement de conformité au RU-18 de la DGPN n'a été transmis à la CNIL que le 14 décembre 2023, soit huit ans après ses premières utilisations.

En troisième lieu, s'agissant de la préfecture de police de Paris, je relève que le logiciel souverain " Système V " est notamment utilisé depuis 2021. Or, je relève que la préfecture de police de Paris a transmis à la CNIL un engagement de conformité concernant la mise en œuvre de ce logiciel le 30 octobre 2023, soit deux ans après le début de son utilisation. Par ailleurs, je relève que, malgré l'utilisation par la préfecture de police de Paris du logiciel " Vidéo Synopsis " (lors de

deux phases d'expérimentation entre 2016 et 2022), du logiciel " Axiom " et du logiciel " Physical Analyzer ", aucun engagement de conformité au RU-18 n'a à ce jour été reçu par la CNIL[14] [↗](#).

Aussi, entre 2015 et les premières transmissions en 2023, et encore récemment pour certains des logiciels, le ministère de l'Intérieur n'a pas respecté les dispositions du décret du 7 mai 2012, en ne transmettant pas d'engagement de conformité à la Commission préalablement à la mise en œuvre de ces logiciels. Dès lors qu'à l'époque le ministère n'analysait pas ces logiciels comme des LRJ, il est par ailleurs probable que les autres dispositions du décret du 7 mai 2012 n'ont pas été bien respectées, notamment en ce qu'elles prévoient une autorisation d'utilisation par un magistrat pour chaque procédure.

Dès lors, en l'absence d'engagement de conformité avant 2023 et en l'absence de décret spécifique les autorisant, certains des logiciels d'analyse vidéo ont été utilisés depuis 2015 en méconnaissance du décret du 7 mai 2012. Il convient en outre de transmettre à la Commission les engagements de conformité au RU-018 encore manquants.

Par ailleurs, je prends note qu'un projet de modification du décret du 7 mai 2012 encadrant les LRJ est actuellement en cours de rédaction, conformément à ce qui a été indiqué dans le cadre des contrôles susmentionnés. Je vous remercie de bien vouloir le finaliser dans les plus brefs délais afin que les traitements d'analyse vidéo y soient explicitement mentionnés.

2. Sur l'obligation d'effectuer une analyse d'impact relative à la protection des données (AIPD)

En droit, l'article 90, paragraphe 1^{er}, de la loi " Informatique et Libertés " dispose que " Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 6 [telles que les " données biométriques aux fins d'identifier une personne physique de manière unique "], le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel ".

De plus, le **considérant 58 de la directive " Police-Justice " précise que " Lorsque des opérations de traitement sont, du fait de leur nature, de leur portée ou de leurs finalités, susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait effectuer une analyse d'impact relative à la protection des données comprenant notamment les mesures, les garanties et les mécanismes envisagés pour assurer la protection des données à caractère personnel et pour apporter la preuve du respect de la présente directive ".**

Ainsi, une évaluation de la nécessité et de la proportionnalité du dispositif envisagé, au regard des finalités poursuivies notamment, doit être opérée avant son implantation.

En l'espèce, dans la réponse au contrôle sur pièces précité, il a été indiqué que le ministère de l'Intérieur utilise des logiciels d'analyse vidéo depuis 2015.

Toutefois, **en premier lieu,** je relève que la DGGN a transmis à la CNIL une AIPD concernant le logiciel " Système V " le 23 novembre 2023 ainsi qu'une AIPD concernant le logiciel " Video Synopsis " de la société BRIEFCAM le 25 octobre dernier seulement, soit six ans après ses premières utilisations[15] [↗](#).

En second lieu, s'agissant de la DGPN, la direction a transmis à la CNIL une AIPD concernant le logiciel " Video Synopsis " de la société BRIEFCAM le 3 janvier 2024, utilisé depuis 2015 par les services de la police nationale, soit près de 9 ans après ses premières utilisations.

Entroisième lieu, je relève que la DPJ-PP a seulement transmis à la CNIL une AIPD concernant l'utilisation du logiciel souverain " Système V ", le 22 novembre 2023. Quant aux autres logiciels de ce type tels que, notamment, le logiciel " Axiom " et le logiciel " Physical Analyzer ", utilisés dans le cadre d'investigations pour le recueil de preuves numériques, la délégation de contrôle a été informée par la préfecture de police de Paris qu'aucune AIPD n'a été réalisée[16] [↗](#).

Or, la mise en œuvre de technologies d'analyse automatisée *a posteriori* des images issues de dispositifs vidéo est susceptible d'entraîner d'importantes conséquences pour les droits et libertés fondamentaux des personnes. La réalisation d'une AIPD avant la mise en œuvre de ces logiciels par le ministère de l'Intérieur aurait permis l'évaluation de tels risques et des mesures proportionnées à ceux liés, notamment, à l'inexactitude des données, à la consultation non-autorisée de ces dernières ou encore à leur perte.

Aussi, de tels traitements n'auraient pas dû être mis en œuvre, ou continué de l'être (l'obligation d'effectuer une AIPD étant prévue depuis le 1^{er} juin 2019, date d'entrée en vigueur des dispositions afférentes de la loi " Informatique et Libertés " telles qu'issues de la transposition de la directive " Police-Justice " par voie d'ordonnance, la CNIL ayant généralement admis un délai de deux ans pour se mettre en conformité avec les nouvelles obligations en matière d'AIPD), sans avoir préalablement fait l'objet d'une AIPD. **Le fait que ces traitements soient menés dans le cadre de phases expérimentales de " tests ", ou qu'ils le soient dans des phases de déploiement opérationnel, est sans incidence sur cette obligation.**

Dès lors, le ministère de l'Intérieur a méconnu les dispositions de l'article 90 de la loi " Informatique et Libertés " en ne réalisant pas d'AIPD préalablement à la mise en œuvre des logiciels d'analyse vidéo, dont notamment ceux de la société BRIEFCAM ainsi que les logiciels souverains " Système V " et " SIGMA ", " Axiom " et " Physical Analyzer ". Vous voudrez bien transmettre l'ensemble des AIPD qui n'auraient pas été transmises à ce jour, notamment " Axiom " ou " Physical Analyzer " pour la préfecture de police de Paris.

3. Sur l'interdiction de principe de mettre en œuvre un traitement de données biométriques aux fins d'identifier une personne physique de manière unique, via un dispositif de reconnaissance faciale notamment

En droit, l'article 34 de la Constitution du 4 octobre 1958 prévoit que " *la loi fixe les règles concernant : (...) les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques (...)* [ainsi que] *la procédure pénale* ".

L'article 88 de la loi " Informatique et Libertés " dispose que le traitement de catégories particulières de données à caractère personnel telles que les données biométriques aux fins d'identifier une personne physique de manière unique " *est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire (...)* ".

Le considérant 51 de la directive " Police-Justice " souligne que " *des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données qui pourraient entraîner des dommages physiques matériels ou un préjudice moral, en particulier (...) lorsque des données (...) biométriques sont traitées afin d'identifier une personne de manière unique (...) ou lorsque (...) des données relatives à (...) des infractions (...) sont traitées ; (...) ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées* ".

Par ailleurs, conformément à l'**article 20 de ladite directive**, les responsables de traitements doivent intégrer les principes de protection des données à caractère personnel en mettant en œuvre toutes les mesures techniques et organisationnelles appropriées et nécessaires, à la fois dès la conception du produit ou du service et par défaut.

Pour rappel, malgré le strict encadrement par le législateur des dispositifs utilisant des données biométriques comme de leurs expérimentations, le développement rapide de nouveaux outils de captation des images et de nouvelles modalités d'exploitation des images de vidéoprotection dans l'espace public, dont la reconnaissance faciale, a poussé la CNIL, en 2018 déjà, à appeler " *d'urgence à un débat démocratique sur cette problématique, et à ce que le législateur puis le pouvoir réglementaire se saisissent de ces questions afin que soient définis les encadrements appropriés, en recherchant le juste équilibre entre les impératifs de sécurisation, notamment des espaces publics, et la préservation des droits et libertés de chacun* "[17] [↗](#). La reconnaissance faciale soulevant des questions inédites touchant à des choix de société, la CNIL a souhaité contribuer au débat qu'elle a appelé de ses vœux en présentant, en 2019, les éléments techniques, juridiques et éthiques devant selon elle être pris en compte dans l'approche de cette question complexe[18] [↗](#).

À ce jour, **les dispositifs d'identification ou de caractérisation des personnes physiques à partir de leurs données biométriques, utilisés de manière opérationnelle comme expérimentale, ne sont pas autorisés par le législateur dans l'espace public.**

En l'espèce, dans la réponse au contrôle sur pièces précité, il a été précisé que " *l'interdiction de toute utilisation d'un quelconque module de reconnaissance faciale a été rappelée par instruction du directeur général [de la Police nationale] du 6 février 2023 adressée à l'ensemble des services utilisateurs (DNSP, DNPJ, SNPS)* ".

Toutefois, **en premier lieu**, lors du contrôle du SCRC-GN, il a été indiqué à la délégation de contrôle qu'une fonctionnalité de " Reconnaissance faciale " avait été intégrée par la société BRIEFCAM lors d'une mise à jour du logiciel, sans demande en ce sens du ministère. Il a été rapporté que cette fonctionnalité de " Reconnaissance faciale " a été utilisée " *une seule fois, lors des émeutes de l'Été 2023* ", semble-t-il pour une recherche *ex post* parmi les images et que, " *à l'usage, la fonctionnalité de " reconnaissance faciale " s'apparente plutôt à une fonctionnalité de similitude d'apparence du fait que celle-ci n'a pas la même efficacité que le module intégré au TAJ et par ailleurs qu'il est possible d'alimenter ce module à partir de la photo d'une personne prise de dos* ". Néanmoins, l'annexe 5 intitulée " Point de situation BRIEFCAM " et datée du 10 janvier 2023, contenue dans le document intitulé " BRIEFCAM_IGA_Annexes 1 à 9.pdf " transmis suite au contrôle, semble indiquer le contraire et confirmer, à cette occasion, une utilisation de ce logiciel à des fins de reconnaissance faciale pour rechercher un individu dans une bande vidéo, dans le cadre d'une enquête judiciaire. Il résulte de ce qui a été dit ci-dessus que cet usage était illégal.

De plus, **en deuxième lieu**, il a été précisé à la délégation de contrôle que, préalablement à la mise à jour du logiciel opérée en 2022 et dans le cadre de laquelle la fonctionnalité " Reconnaissance faciale " est apparue, une fonctionnalité intitulée " Similitudes d'apparence " lui préexistait. Le matériel du SCRC-GN ayant été désinstallé au mois de mars 2024, ladite délégation n'a pu effectuer aucune constatation lors du contrôle effectué en mai dernier.

Enfin, **en troisième lieu**, si la désinstallation du logiciel de la société BRIEFCAM a été ordonnée au sein de la gendarmerie nationale, tel n'a pas été le cas dans l'ensemble des services du ministère de l'Intérieur. Aussi, je relève que des fonctionnalités s'apparentant à des traitements biométriques sont toujours disponibles au sein des logiciels mis en œuvre par des services relevant du ministère de l'Intérieur, et que leur usage reste ainsi techniquement possible, du moins en théorie.

Or, je vous rappelle que la distinction entre les dispositifs biométriques et non biométriques a des conséquences juridiques importantes : les dispositifs biométriques impliquent des traitements de données dites " sensibles " qui sont, par principe, interdits par la loi " Informatique et Libertés " comme le RGPD, sauf exceptions. Il vous appartient, en tant que responsable de traitement, de vous assurer que ce type de traitement ne repose pas sur l'utilisation de données biométriques.

La fonctionnalité " Reconnaissance faciale " semblant être activée par défaut par certains éditeurs (au sein des logiciels de la société BRIEFCAM notamment), j'estime que le respect des textes cités ci-dessus implique que le ministre de l'Intérieur prenne des mesures pour empêcher l'utilisation de cette fonctionnalité, par exemple en prévoyant la désactivation par un compte " administrateur ", afin qu'elle ne puisse pas être mise en œuvre par les utilisateurs du logiciel, ainsi qu'une remontée d'alerte automatique au responsable de traitement en cas de réactivation. Idéalement, une version spécifique du logiciel n'intégrant pas ce type de fonctionnalité devrait être privilégiée (comme cela est désormais prévu par la société BRIEFCAM^[19] [↗](#)).

Dès lors, le ministère de l'Intérieur a méconnu les dispositions de l'article 88 de la loi " Informatique et Libertés " :

- du fait de l'usage de la fonctionnalité de reconnaissance faciale lors d'une procédure à l'été 2023 ;
- plus généralement, en ne prenant pas de mesures de nature à empêcher l'utilisation de la fonctionnalité de reconnaissance faciale au sein des logiciels d'analyse vidéo qui proposent cette fonctionnalité par défaut, en particulier les logiciels de la société BRIEFCAM.

Enfin, au vu de ces éléments, je vous rappelle la nécessité, dans le cadre du développement du logiciel souverain " Système V " comme de tout autre logiciel développé par vos services, de garantir le respect des règles de protection des données à caractère personnel dès sa conception et par défaut, en n'incluant aucune fonctionnalité basée sur des données biométriques.

II- Mesures correctrices prononcées par la CNIL

En raison de l'ensemble de ces éléments et conformément aux dispositions de l'article 20 de la loi " Informatique et Libertés ", il y a donc lieu de prononcer à l'égard du MINISTÈRE DE L'INTÉRIEUR, les mesures correctrices suivantes :

- Un **RAPPEL AUX OBLIGATIONS LÉGALES**, pour avoir utilisé des logiciels d'analyse vidéo (*logiciels de rapprochement judiciaire*) sans transmission préalable à la CNIL des engagements de conformité correspondants, dans les conditions rappelées ci-dessus, ce qui méconnaît les articles 4 et 31 de la loi " Informatique et Libertés ".
- Une **MISE EN DEMEURE**, sous un délai de deux (2) mois à compter de la notification de la présente décision et sous réserve des mesures qu'il aurait déjà pu adopter :
- **de transmettre des engagements de conformité au règlement unique RU-018 pour les différents logiciels de rapprochement judiciaire (LRJ) mis en œuvre n'en ayant encore pas fait l'objet**, conformément aux dispositions des articles 31 de la loi " Informatique et Libertés " et 6 du décret du 7 mai 2012. Cela concerne notamment le logiciel " Physical Analyzer " et le logiciel " Axiom " mis en œuvre par la préfecture de Police de Paris. Dans l'hypothèse où le ministère aurait cessé l'utilisation de l'un ou plusieurs LRJ évoqués dans le cadre de la procédure de contrôle susmentionnée, il convient d'en informer la CNIL en réponse à la présente mise en demeure ;
- **deréaliser une analyse d'impact relative à la protection des données (AIPD)** pour les différents LRJ n'en disposant pas encore, notamment les logiciels " Physical Analyzer " et " Axiom ", conformément aux dispositions des articles 90 de la loi " Informatique et Libertés " et 6 du décret du 7 mai 2012 ;
- **de prendre les mesures adéquates permettant d'empêcher, conformément au cadre légal, l'utilisation des fonctionnalités de reconnaissance faciale pour l'ensemble des LRJ utilisés;**
- **de justifier auprès de la CNIL que l'ensemble de ces demandes a bien été respecté, dans le délai imparti.**

À l'issue de ce délai, si le ministère de l'Intérieur s'est conformé à la présente mise en demeure, la procédure sera close et un courrier sera adressé en ce sens.

À l'inverse, en l'absence de respect de la mise en demeure, il est rappelé que la présidente de la CNIL peut désigner un rapporteur pour requérir que la formation restreinte prononce l'une des sanctions prévues à l'article 20 de la loi du 6 janvier 1978.


Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.


[...]


La Présidente


Marie-Laure DENIS

[...]


[1]  Analyse algorithmique des images de vidéos en temps différé et non pas en temps réel (à ce sujet, *confer* position de la CNIL de juillet 2022 sur les conditions de déploiement des caméras dites intelligentes ou augmentées dans les espaces publics).


[2]  Articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 et 99-4 du code de procédure pénale (CPP).


[3]  Art. 230-20 et suivants et R. 40-39 à R. 40-41 du CPP.


[4]  *dossier technique* dans le décret n° 2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle (ci-après, décret du 7 mai 2012), concernant lequel la Commission a rendu un avis en prenant acte de l'engagement du ministère de l'intérieur à joindre à ces engagements de conformité des dossiers techniques précisant notamment les fonctionnalités exactes de chaque logiciel, son architecture technique ainsi que les mesures de sécurité encadrant le traitement projeté et soulignant qu'elle s'attacherait tout particulièrement, à l'occasion de la fourniture des dossiers de présentation technique des logiciels qui seront ultérieurement déclarés, à vérifier que l'utilisation de ces logiciels est limitée à l'échelon local dans le cadre d'une procédure judiciaire spécifique (délibération n° 2011-418 du 15 décembre 2011 portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle).


[5]  Art. 6 du décret du 7 mai 2012.


[6]  Art. 230-23 du CPP.


[7]  COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, Délibération n° 2011-418 du 15 décembre 2011 portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle.


[8]  <https://www.cnil.fr/fr/declaration/acte-reglementaire-unique-18-logiciel-de-rapprochement-judiciaire-des-fins-danalyse-criminelle>


[9]  Art. 230-20 du CPP.


[10]  Conformément à l'article R. 40-40 du CPP, ledit magistrat doit **autoriser** l'exploitation d'enregistrements vidéo par le biais d'un LRJ pour chaque procédure qu'il contrôle. Cette autorisation, comme la mise en œuvre elle-même, doivent faire l'objet d'une **mention en procédure** et, à la clôture de cette dernière, un **rapport d'exploitation** des données doit y être joint.


[11]  Permettant un gain de temps de visionnage par la compression des temps morts ainsi que la détection d'un objet ou d'une personne, grâce [à] différents filtres (couleur, forme d'objet, direction, arrêt près de telle zone sélectionnée), plaques minéralogiques, similitudes d'apparence (reconnaissance de formes d'une silhouette similaire grâce à une photo) (PV 2023-259/2 du 21 mai 2024).

[12]  Outil d'analyse souverain développé par le département des technologies appliquées à l'investigation D@TA-i de la direction nationale de la police judiciaire (DNPJ) et ayant vocation à être déployé de manière généralisée.


[13]  Les engagements de conformité au RU-18 des logiciels suivants – ne rentrant pas dans le cadre des constatations effectuées lors des contrôles sur place menés par la CNIL – ont également été reçus : la DGGN a transmis à la CNIL deux engagements de conformité concernant respectivement le logiciel LARC (le 27 juillet 2023) et le logiciel DA-DT (le 28 juillet 2023), qui ne sont pas des logiciels d'analyse vidéo.


[14]  Les engagements de conformité au RU-18 des logiciels suivants – ne rentrant pas dans le cadre des constatations effectuées lors des contrôles sur place menés par la CNIL – ont également été reçus : la DGPN a transmis à la CNIL, le 20 juillet 2023, deux engagements de conformité concernant respectivement le logiciel souverain Système V et le logiciel Pathfinder de la société CELLEBRITE, ainsi qu'un engagement relatif au logiciel souverain SIGMA le 23 mai 2024.


[15]  Les AIPD des logiciels suivants – ne rentrant pas dans le cadre des constatations effectuées lors des contrôles sur place menés par la CNIL – ont également été reçus : la DGGN a transmis à la CNIL deux AIPD concernant respectivement le logiciel LARC et le logiciel DA-DT (le 9 janvier 2024), qui ne sont pas des logiciels d’analyse vidéo.

[16]  La DGPN a transmis à la CNIL sans AIPD les engagements de conformité concernant respectivement le logiciel souverain Système V et le logiciel Pathfinder de la société CELLEBRITE – ne rentrant pas dans le cadre des constatations effectuées lors des contrôles sur place menés par la CNIL.

La DGPN a transmis à la CNIL le 11 juillet 2024 une AIPD concernant le logiciel souverain SIGMA .

[17]  <https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video>

[18]  <https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux>

[19]  Communiqué de presse de la société BRIEFCAM publié le 12 décembre 2023 sur son site web indiquant qu’ *Avec la sortie de 2024 M1, BriefCam introduit la flexibilité d’implémenter une licence en excluant la capacité de reconnaissance faciale. Conçue pour étendre la puissante technologie BriefCam aux organisations soumises à des restrictions strictes en matière d’utilisation de la reconnaissance faciale, BriefCam a développé sa solution pour mieux répondre aux besoins réglementaires internationaux et en constante évolution. Les utilisateurs de BriefCam peuvent passer à une version où la reconnaissance faciale est complètement désactivée et exclue de l’interface utilisateur et des algorithmes. .*