RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

CONFIDENTIEL

Usage de logiciels d'analyse vidéo par les services de la police et la gendarmerie nationales

INSPECTION GENERALE
DE LA POLICE NATIONALE

N° 23-00779-I

INSPECTION GENERALE
DE L'ADMINISTRATION

N° 23114-R

INSPECTION GENERALE
DE LA GENDARMERIE NATIONALE

N° 939

- Février 2024 -

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

INSPECTION GENERALE DE LA POLICE NATIONALE	INSPECTION GENERALE DE L'ADMINISTRATION	INSPECTION GENERALE DE LA GENDARMERIE NATIONALE
N° 23-00779-I	N° 23114-R	N° 939

CONFIDENTIEL

Usage de logiciels d'analyse vidéo par les services de la police et la gendarmerie nationales

Établi par

Fabienne DUTHE
Commissaire générale,
inspection générale de la police nationale

Pascal GIRAULT
Inspecteur général de l'administration

Jean-Marc TEISSIER
Colonel, inspection générale de la gendarmerie nationale

Daniel MONTIEL
Commissaire général,
inspection générale de la police nationale

Anne CORNET
Inspectrice générale de l'administration

Christophe BAUDRY
Colonel, inspection générale de la gendarmerie nationale

- Février 2024 -

SYNTHESE

Le 14 novembre 2023, l'organisme d'investigation Disclose faisait état d'une utilisation illégale par la police nationale, depuis 2015, d'un *« logiciel israélien de reconnaissance faciale »* édité par la société *BriefCam*, qui serait utilisé *« dans le plus grand secret ».* Depuis huit ans, la reconnaissance faciale serait ainsi *« activement utilisée sans contrôle ni réquisition judiciaire »*.

A la suite de cet article, la Commission nationale de l'informatique et des libertés (CNIL) a diligenté, le 6 décembre 2023, un contrôle sur pièces du respect par le ministère de l'intérieur du droit de la protection des données. Le ministre a annoncé, pour sa part, une enquête interne.

C'est dans ce contexte que le directeur du cabinet du ministre de l'intérieur et des outre-mer a demandé, le 24 novembre 2023, à l'inspection générale de l'administration, à l'inspection générale de la police nationale et à l'inspection générale de la gendarmerie nationale d'étudier l'utilisation de logiciels d'analyse vidéo par les services de police et de gendarmerie et le respect du cadre légal de ces utilisations, notamment pour la reconnaissance faciale. Des propositions touchant au contrôle interne sont également souhaitées, prenant en compte les innovations technologiques dont peuvent avoir besoin les forces de sécurité pour l'exercice de leurs missions.

Conformément à ce mandat, la mission s'est concentrée sur l'utilisation des logiciels d'analyse vidéo par les services de police et de gendarmerie, à l'exclusion des services de renseignement, d'une part, et des polices municipales, d'autre part. S'agissant de ces dernières, elle s'est cependant intéressée, pour une bonne compréhension de la thématique étudiée, aux relations pouvant exister entre ces services municipaux et les forces de sécurité de l'Etat en matière d'exploitation d'images vidéo.

La mission observe d'abord que le recours aux logiciels d'analyse vidéo par les forces de sécurité est une réponse à l'impérieuse nécessité, pour ces services, de sélectionner dans les flux considérables d'images vidéo produites chaque jour - avec le soutien puissant des pouvoirs publics s'agissant des caméras de voie publique - les seules images utiles aux actions dont ils sont légalement chargés, que ce soit en police judiciaire ou en police administrative. Les flux vidéo sont tels que leur exploitation est désormais impossible sans une aide numérique.

Eu égard à cette nécessité, les conditions d'acquisition du logiciel *BriefCam*, dès 2015 dans la police et 2017 dans la gendarmerie interrogent. Si la finalité de cette acquisition est univoque (le logiciel n'a été acquis et déployé que pour un usage exclusivement judiciaire et non en police administrative, et pour une exploitation en temps différé et non en temps réel), elle s'est faite en ordre dispersé par les forces et au sein des forces, sans que le besoin soit réellement formalisé. Ce n'est qu'*a posteriori* qu'on peut dégager deux lignes directrices : en police, une affectation prioritaire dans les services de soutien et d'assistance techniques, plutôt qu'auprès des enquêteurs de terrain ; en gendarmerie, une vocation de traitement de la criminalité du « haut du spectre » plutôt que de la délinquance du quotidien. Les services affectataires sont restés très peu nombreux : au total, 57 licences seulement sont opérationnelles à la date de ce rapport. Les utilisations effectives du logiciel depuis 2015 sont quant à elles rares, interrogeant même sur le retour sur investissement d'un logiciel onéreux, même si l'utilité des logiciels d'analyse vidéo ne peut se résoudre à une simple équation comptable. Car c'est surtout à la méconnaissance générale, dans les services, de l'existence de cette solution numérique, plus qu'à un doute sur son utilité opérationnelle intrinsèque, qu'il convient d'imputer ce faible taux d'utilisation.

Le temps nécessaire à l'identification du statut juridique de ce type de logiciel est une autre source d'interrogation. Huit ans ont été nécessaires avant que *BriefCam* soit officialisé comme un logiciel de rapprochement judiciaire (LRJ) au sens du code de procédure pénale et du décret du 7 mai 2012 réglementant ces logiciels, huit ans pendant lesquels il est resté un objet juridique non identifié, alors que les LRJ, au nombre desquels il a donc été finalement rangé, ont un statut précis en procédure pénale, leur usage étant soumis à l'autorisation préalable du juge et devant être

mentionné en procédure. Un tel délai, s'il s'explique par plusieurs facteurs, appelle pour l'avenir des mesures correctives relevant du contrôle interne sur l'acquisition sur le marché de ce type de produit. L'analyse juridique doit se faire *ab initio* et être globale, comme l'expertise technique, au regard des enjeux de sécurité numérique ministérielle et de cohérence d'équipement des directions-métier. A l'heure où le développement de l'intelligence artificielle (IA) va multiplier les offres de solutions numériques sur le marché, dont certaines présenteront à n'en pas douter un intérêt opérationnel pour les forces de sécurité, l'ensemble du processus d'achat doit donc être maîtrisé et contrôlé, évidemment au regard des règles de la commande publique, mais aussi au regard de statut juridique de ces solutions et de leurs caractéristiques techniques.

S'agissant de la problématique de la reconnaissance faciale, la mission rappelle que le logiciel *BriefCam* n'a été utilisé par la police et la gendarmerie nationales que dans un cadre strictement judiciaire et toujours en temps différé. Ensuite, le logiciel n'a pas été acheté ni déployé dans l'intention de mettre en œuvre de la reconnaissance faciale puisque cette fonctionnalité n'existait pas lors des acquisitions initiales. Elle n'a été introduite, à l'initiative de l'éditeur, qu'à partir de novembre 2018, postérieurement aux décisionsd'acquisition. Seules donc les licences acquises ou renouvelées depuis cette date comportent cette fonctionnalité, qui repose sur une technologie biométrique. La reconnaissance faciale n'a donc ni motivé l'achat du logiciel, ni suscité de demandes de la part des services, pour lesquels elle présente au demeurant peu d'intérêt eu égard aux modes opératoires habituels des auteurs d'infractions graves (dissimulation de visage).

Pour vérifier d'éventuelles utilisations de la reconnaissance faciale depuis novembre 2018, la mission s'est appuyée sur les déclarations des services, dont elle a acquis la certitude de la bonne foi, qui sont la seule source d'information exploitable, puisque les « logs » de connexion au logiciel sont effacés au bout de 365 jours et qu'ils ne détaillent pas l'activation des différentes fonctionnalités du logiciel. Dans ce contexte déclaratif, un cas unique d'activation dans une procédure judiciaire de la fonctionnalité de reconnaissance faciale - qui n'a conduit à aucune mise en cause de personnes suspectées - a été porté à la connaissance de la mission. Unique, ce cas est évidemment de trop puisqu'il se situe hors cadre légal. Son unicité vient toutefois en contrepoint de l'affirmation d'une fonctionnalité *« activement utilisée »*.

Au-delà des constats, la mission relève l'insuffisante coordination des deux forces dans la gestion administrative du dossier *BriefCam*, nuisant à la cohérence et à l'intelligibilité de l'action du ministère. Elles ont fait des choix différents de régularisation de ce traitement auprès de la CNIL en tant que LRJ. Le rappel pédagogique d'interdiction formelle de recours à la reconnaissance faciale dans ce type de logiciel n'a été fait que par une seule direction générale. Le maintien, à la date du rapport, d'un régime de suspension d'utilisation du logiciel par les enquêteurs, alors même qu'il est désormais administrativement régularisé, paraît difficilement compréhensible et risque surtout de nuire à la conduite d'enquêtes judiciaires de plus en plus souvent tributaires de l'exploitation de très importants flux d'images. Le maintien d'une telle suspension serait d'autant plus problématique que la solution souveraine *Système V*, qui se substituera à *BriefCam* ne sera pas opérationnelle à court terme.

Enfin, *BriefCam* illustre le besoin, qui ira croissant avec le développement de l'IA, d'expérimentation par les forces de sécurité de nouvelles solutions numériques, de plus en plus nombreuses sur un marché plus créatif et agile que les Etats, dont certaines offriront à n'en pas douter des réponses utiles aux besoins opérationnels des services. L'entrée en vigueur du Règlement européen sur l'IA, en cours de finalisation, offrira à cet égard des opportunités d'évolutions structurantes de la loi « informatique et libertés ». L'introduction dans ce texte d'un dispositif-cadre d'expérimentation de nouvelles solutions numériques, tout particulièrement par les forces de sécurité, est une nécessité dont ce Règlement offre une opportunité de traduction normative. Une réflexion devrait donc être rapidement engagée pour donner un cadre à de telles expérimentations, en allégeant, dans le respect de garanties intangibles pour les libertés et dans la transparence, le dispositif d'autorisation réglementaire des traitements de souveraineté, qui, très contraignant, s'inscrit surtout dans un temps long incompatible avec le concept même d'expérimentation.

TABLE DES RECOMMANDATIONS PRIORITAIRES

PRIORITES	DESTINATAIRES	RECOMMANDATIONS
1	DGPN	Lever sans délai la suspension d'utilisation du logiciel *BriefCam* par les services enquêteurs de la police nationale (recommandation n°6)
2	DGPN ; DGGN	Poursuivre l'utilisation du logiciel *BriefCam* dans les services d'enquête, jusqu'à son remplacement par le logiciel *Système V* (recommandation n°7)
3	DGPN ; DGGN	Assurer une unité de doctrine de la police et de la gendarmerie nationales sur la définition du cadre juridique des nouvelles technologies numériques et sur leur doctrine d'emploi (recommandation n°5)

Liste des recommandations par ordre d'apparition dans le rapport

SOMMAIRE

INTRODUCTION

Par lettre de mission du 24 novembre 2023, le directeur de cabinet du ministre de l'intérieur et des outre-mer a diligenté une mission inter-inspections (inspection générale de l'administration, inspection générale de la police nationale, inspection générale de la gendarmerie nationale) relative à la mise en œuvre de logiciels algorithmiques d'analyse vidéo par les services de la police et de la gendarmerie nationales. Cette mission fait suite à la publication, le 14 novembre par un organisme d'investigation, d'un article faisant état de l'utilisation par la police nationale, depuis 2015, du logiciel de la société israélienne *BriefCam*, permettant l'usage par ces services de la reconnaissance faciale en dehors de tout cadre légal. La CNIL, postérieurement à cette publication, a décidé de son côté un contrôle sur pièces du respect par le ministère de l'intérieur du droit des données personnelles dans l'usage de ce logiciel.

Il est demandé à la mission :

- de vérifier les cas d'utilisation de ce type de logiciels au sein des services d'investigation, de dresser la liste des unités utilisatrices et leur degré d'utilisation ;

- de s'assurer que les fonctionnalités de reconnaissance faciale n'ont pas été mises en œuvre et que l'utilisation des logiciels ne s'est faite, sous l'autorité d'un magistrat, que dans un cadre judiciaire.

La mission est par ailleurs invitée à faire des propositions d'amélioration du contrôle interne dans la mise en œuvre de dispositifs technologiques expérimentaux pour s'assurer du respect du cadre légal, sans proscrire l'esprit d'innovation.

La mission a tout d'abord procédé à un recensement auprès des directions générales de la police et de la gendarmerie ainsi que de la préfecture de police de Paris, des services dotés de *BriefCam* ou de logiciels équivalents, complété de la chronologie des déploiements, des références de licences informatiques acquises et des cas d'usage. L'absence de traçabilité informatique exploitable depuis 2015 de l'usage du logiciel ne laissait en effet d'autre choix que de solliciter des remontées d'information et de documentation de la part des services utilisateurs. Les informations recueillies sont évidemment tributaires de la rigueur du suivi de ce logiciel par les services depuis près de 10 ans, et de la mémoire des agents actuellement présents dans les unités concernées. La mission n'est donc pas en mesure de s'appuyer sur un état objectif et exhaustif de ces données, ce qui ne l'empêche pas de fonder ses observations sur un nombre important d'informations dont la fiabilité est à l'aune de leur cohérence.

Ensuite, la mission a procédé à une trentaine d'entretiens, tant au niveau central qu'avec des services territoriaux utilisateurs, de la police et de la gendarmerie. Elle a également eu des échanges avec la Commission nationale de l'informatique et des libertés (CNIL), dans le respect de l'indépendance des missions de contrôle de cette dernière et d'inspection de la mission, et avec des membres du Conseil d'Etat. La mission a également rencontré le distributeur en France, pour les forces de sécurité, du logiciel *BriefCam* et échangé avec l'éditeur du logiciel.

Au terme de ces démarches, la mission souligne d'abord le caractère absolument indispensable du recours aux logiciels d'analyse vidéo pour les activités opérationnelles des services de police et de gendarmerie reposant sur l'exploitation des flux vidéo, même si la politique d'achat et de déploiement a souffert d'un relatif désordre (partie 1). Elle analyse ensuite les conditions dans lesquelles le statut juridique du logiciel a, très tardivement, été identifié et officialisé et la réalité de la fonctionnalité de reconnaissance faciale dans ce logiciel et de son usage par les forces (partie 2). Elle propose enfin des pistes de sécurisation de la mise en œuvre de nouvelles solutions numériques par les forces de sécurité et de définition d'un cadre légal d'expérimentation de telles solutions numériques, dont la mise en œuvre du Règlement européen sur l'intelligence artificielle offre l'opportunité (partie 3).

1 UN LOGICIEL D'UNE UTILITE CERTAINE, ACQUIS POUR UN USAGE JUDICIAIRE SANS VISION STRATEGIQUE

Depuis le début des années 2000, l'image connaît une croissance considérable et continue. Elle est produite et diffusée en masse par les personnes physiques. Les données générées par un individu doubleraient ainsi tous les deux ans. Mais les personnes morales et les institutions participent également à ce phénomène. Selon la direction des entreprises et partenariats de sécurité et des armes (DEPSA) du ministère de l'intérieur, la France compterait aujourd'hui plus de 1 110 000 caméras de vidéoprotection autorisées dans l'espace public, dont 10% environ sur les voies publiques, lesquelles sont principalement installées, avec le soutien résolu de l'Etat, par les communes et les intercommunalités. En 2020, 60% se trouvaient en zone police, 40% en zone gendarmerie. Ce parc génère, chaque jour, plusieurs millions d'heures d'images vidéo.

Ces images, toutes origines confondues, constituent des données qui, si elles doivent être exploitées, deviennent un enjeu majeur pour les forces de sécurité intérieure de l'État. Elles peuvent potentiellement être traitées soit en temps réel, en police administrative, soit en temps différé, pour les besoins des enquêtes judiciaires.

A cet égard, en dépit du fait que, comme le relève à juste titre la Cour des comptes[1], le code de la sécurité intérieure (CSI) ne mentionne pas l'élucidation de faits à des fins judiciaires comme étant au nombre des finalités des systèmes de vidéoprotection, énumérées par l'article L.251-2[2], l'utilisation d'images issues de la vidéoprotection est désormais indispensable aux services enquêteurs.

C'est pour répondre à la nécessité absolue de réduire l'écart entre le volume d'images brutes issues de systèmes vidéo, quelle qu'en soit l'origine, pouvant nourrir l'enquête et la capacité humaine à les exploiter, que la police et la gendarmerie nationales ont acquis sur le marché, respectivement en 2015 et 2017, dans un but exclusif d'utilisation dans un cadre judiciaire, le logiciel d'analyse vidéo *BriefCam*.

1.1 Les logiciels d'analyse vidéo sont devenus indispensables à l'enquête judiciaire

1.1.1 L'aide numérique à l'exploitation des images : une nécessité résultant de la croissance continue des flux vidéo

1.1.1.1 La vidéoprotection s'est généralisée avec l'encouragement et le soutien actif de l'Etat

L'augmentation constante, depuis la loi du 21 janvier 1995[3] qui l'a autorisée, de la couverture de l'espace public en caméras de surveillance vidéo est le fruit d'une politique volontariste de l'Etat, régulièrement affirmée[4], confortée par l'inscription de ces matériels au catalogue de l'Union des groupements d'achats publics (UGAP)[5], portée par un discours politique fortement incitatif à

[1] « Le plan de vidéoprotection de la préfecture de police de Paris » Référé 2 décembre 2021, point 4-1

[2] Cf. article L.251-2 du CSI. Toutefois, selon l'article 427 du code de procédure pénale, *« hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve »*, au nombre desquels figurent les images vidéo.

[3] Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

[4] Le 30 juillet 2007, par exemple, la lettre de mission du président de la République charge la ministre de l'intérieur de *"déployer plus de moyens de vidéosurveillance, qui sont un instrument essentiel de prévention et de répression des actes terroristes"*. Plus récemment, le rapport annexé à la loi d'orientation et de programmation du ministère de l'Intérieur et des outre-mer du 24 janvier 2023 indique (point 2.8) que *« les crédits du fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR) consacrés à la vidéoprotection seront triplés sur les cinq années à venir et viendront cofinancer les projets portés par les collectivités »*.

5 L'acquisition des matériels de surveillance vidéo est en effet facilitée par leur disponibilité au catalogue de l'UGAP. Elle s'étend - dans une démarche générale initiée en 2013 d'offre par l'UGAP de solutions logicielles, tous domaines confondus -, à des logiciels d'exploitation des images vidéo, d'ailleurs sans attention spécifique portée au cadre juridique de leur utilisation. Les acheteurs sont en effet considérés comme professionnels et demeurent responsables de ces vérifications. Seules les documentations commerciales des éditeurs sont fournies aux acheteurs par l'UGAP.

l'adresse des élus municipaux[6], et complétée d'un soutien budgétaire conséquent, auquel participent par ailleurs très largement - quoique dans des conditions de légalité contestables eu égard à leurs compétences[7] - des régions et des départements.

Entre 2010 et 2017, l'Etat a, pour sa part, subventionné à hauteur de 118 M€[8] l'installation de caméras sur la voie publique par les collectivités locales, prioritairement par une mobilisation systématique du fonds interministériel de prévention de la délinquance (FIPD) géré par le comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR). 11,6 M€ y ont été consacrés en 2020, 14 M€ en 2021, près de 19 M€ en 2022, 30 M€ en 2023[9], avec des taux de subventionnement allant, pour cette seule source de financement, de 20 à 50%.

D'autres concours financiers de l'Etat complètent ce financement : la dotation de soutien à l'investissement local (DSIL), la dotation d'équipement des territoires ruraux (DETR) et la dotation politique de la ville (DPV). Entre 2018 et 2022, 2 236 projets ont été cofinancés par l'Etat à travers ces dernières dotations[10], à hauteur de plus de 69 M€, avec un effet de levier sur l'investissement en dispositifs communaux ou intercommunaux de vidéoprotection d'environ 2,5. Toutes sources de concours financiers confondues, le subventionnement peut atteindre 80%.

Les fonds de concours de l'Agence du recouvrement des avoirs saisis et confisqués (AGRASC) et de la Mission interministérielle de lutte contre les drogues et les conduites addictives (MILDECA) peuvent également compléter, ponctuellement, les subventions de l'Etat. Depuis 2015, pour une meilleure synergie des politiques publiques, le FIPD et le fonds de concours de la MILDECA peuvent être ainsi sollicités sur un même projet, les circuits de validation demeurant autonomes.

Enfin, l'État contribue à l'équipement de protection vidéo d'acteurs privés comme les buralistes, avec des aides à la sécurité des débits de tabacs[11].

Au bénéfice de ces aides financières massives, plus de 6 000 communes sont aujourd'hui dotées de caméras dans l'espace public, 30 000 nouvelles caméras étant installées chaque année.

Au-delà des chiffres, les instructions d'utilisation du FIPD apportent d'intéressantes précisions sur la nature des équipements subventionnables. Rompant avec la pratique antérieure, qui considérait comme éligibles à ce fonds les seuls projets d'installation de caméras sur la voie publique ainsi que la création des centres de supervision urbains (CSU) et leur raccordement aux forces de sécurité de l'Etat[12], la circulaire du 5 mars 2020[13] (qui indique par ailleurs que la vidéoprotection « *peut (…) permettre aux enquêteurs de s'appuyer sur les images enregistrées dans le cadre d'une enquête judiciaire »,* prenant acte de la place des images de vidéoprotection dans les enquêtes) dispose que

[6] *« La vidéoprotection est un outil essentiel pour renforcer la sécurité de lieux sensibles tels que les écoles, les lieux de culte, et de rassemblement. J'appelle les collectivités locales à accélérer la mise en place de ces dispositifs. L'État sera pleinement à leurs côtés »* (S. AGRESTI-ROUBACHE, secrétaire d'État chargée de la citoyenneté et de la ville ; communiqué de presse 18 octobre 2023).

[7] TA de Marseille, 17 décembre 2019, n° 1703337 : *« Eu égard au périmètre de la compétence* [de] *la collectivité régionale, la région Provence-Alpes-Côte d'Azur n'est pas fondée à faire valoir que le financement d'équipements (…) de vidéo-protection (…)* [au bénéfice de communes] *pourrait être directement rattaché à la compétence qui lui est attribuée en matière d'aménagement du territoire »*

[8] Données DEPSA.

[9] Toutefois, cette somme de 30 M€ comprend également les équipements des polices municipales.

[10] Source DGCL.

[11] L'accord entre le ministre des comptes publics et la confédération des buralistes conclu le 19 janvier 2023 pour la période 2023-2027 reconduit l'aide antérieure à la sécurité des buralistes, plafonnée à 10 000 € tous les 5 ans. Celle-ci permet un financement forfaitaire de l'installation et du renouvellement de dispositifs de vidéosurveillance (système vidéo, écran et caméras dans la limite de 5).

[12] Cf par ex. Annexe 7 de l'instruction SG-CIPDR *Orientations pour l'emploi des crédits du FIPD pour 2018* (3 mai 2018). L'instruction du 16 février 2023, priorise de son côté le financement des équipements communaux de transferts d'images vers les services de police et les unités de gendarmerie, *« ainsi que l'équipement des forces de sécurité de l'Etat, sous la forme de terminaux nécessaires à leur exploitation »*. Précisons à cet égard que les logiciels d'analyse vidéo n'ont, par construction, jamais été considérés comme des *« terminaux nécessaires »* à l'exploitation des images vidéo des communes. Comme on le verra, aucune acquisition de ce type de logiciel n'a donc été financée par ce canal.

[13] Circulaire SG-CIPDR INTA2006736C.

« *pourront être soutenus (…)* ***les logiciels d'aides à la décision ou aux levées de doute***[14] *».* Plus précise encore, l'instruction du 30 avril 2021[15] pousse à *« expérimenter* ***le traitement automatisé de l'image****, dans les limites rappelées par la SNPD*[16]*, par exemple grâce à des* ***logiciels de détection des situations comportant un danger manifeste*** *(mouvement de foule inhabituel, intrusion dans un espace interdit, départ d'incendie etc.) ».* Enfin, le livret pratique de la direction des coopérations de sécurité (DCS), à laquelle a succédé la DEPSA, accompagnant les instructions FIPD annuelles, mentionnait la possible éligibilité des acquisitions de logiciels au subventionnement FIPD, sans toutefois en préciser la nature.

A la suite de l'étude de la CNIL sur les *« dispositifs constitués de logiciels de traitements automatisés d'images associés à des caméras,* [permettant] *d'extraire diverses informations à partir de flux vidéo qui en sont issus »*, dits « caméras augmentées » ou « intelligentes »[17], concluant qu'ils ne peuvent être autorisés que par la loi, l'instruction du 16 février 2023[18] ne mentionne plus, parmi les équipements subventionnables, les logiciels de détection de situations à danger manifeste[19]. Le CIPDR depuis cette date, a par ailleurs demandé aux communes d'attester, à l'appui de leur demande de subvention, qu'elles n'utilisent aucun dispositif de cette nature.

1.1.1.2 L'importance des flux vidéo impose une aide à leur exploitation

Dans ce contexte de soutien puissant des pouvoirs publics au développement de la vidéoprotection, deux raisons majeures expliquent la nécessité pour les enquêteurs de disposer d'une aide numérique à l'exploitation des flux vidéo faisant l'objet de réquisitions judiciaires.

En premier lieu, l'augmentation considérable de la volumétrie des données numériques[20] crée mécaniquement une contrainte nouvelle sur la capacité des services d'enquête à les exploiter. Si, dans la majorité des cas, cette exploitation peut être faite « manuellement » par l'enquêteur, dans certaines affaires, le volume d'images vidéo à analyser est tel qu'il ne peut plus être traité dans un temps compatible avec les exigences de l'enquête. Dans ces situations, l'utilisation d'un logiciel d'analyse vidéo devient une impérieuse nécessité, et même une condition *sine qua non* de la capacité d'exploitation de cette source d'informations pouvant contribuer à l'établissement de la preuve, surtout lorsque la victime est en danger immédiat de mort ou a disparu.

[14] Surligné par la mission.
[15] Instruction ministérielle INTK2111639J.
[16] Le livret de la stratégie nationale de prévention de la délinquance (SNPD) 2020-2024 comporte, sous la mesure 26 (*"En matière de vidéoprotection : expérimenter le traitement automatisé de l'image, dans le respect des libertés individuelles »),* une action 26-1 *: « Tester la connexion de logiciels de détection comportant un danger manifeste, à l'exclusion de tout traitement permettant l'identification directe ou indirecte des personnes physiques (article L. 251-1 du CSI) »*
[17] CNIL : *« Caméras dites « intelligentes » ou « augmentées » dans les espaces publics »*, juillet 2022
[18] Instruction ministérielle IOMK2303419J du 16 février 2023 *relative aux orientations des politiques soutenues par le FIPD pour 2023.*
[19] L'instruction confirme par ailleurs les instructions précédentes sur le non financement des équipements de vidéo-verbalisation par lecture automatisée de plaques d'immatriculation (LAPI), qui, d'une part, ne concernent pas la prévention de la délinquance et, d'autre part, ne sont pas autorisés pour les communes, selon l'analyse de la CNIL.
[20] Dans le monde, les données numériques ont été multipliées par 50 entre 2010 et 2020 dont une partie seulement sont générées par des dispositifs de vidéoprotection et de vidéosurveillance. Les services d'enquête exploitent également, sur réquisition judiciaire, de nombreuses vidéos issues de webcams, de caméras mobiles, de téléphones ou des applications de messagerie instantanée.

Encadré n°1 : quatre illustrations de volumétrie des flux vidéo dans des enquêtes judiciaires

- Dans le cadre de l'affaire du terroriste Mohamed MERAH, en 2012, 35 téraoctets (To) de données vidéo ont été saisies. Un an et demi a été nécessaire à un enquêteur de la sous-direction anti-terroriste (SDAT) de la DCPJ, avec l'aide du service national de la police scientifique (SNPS) pour visionner « manuellement », sans assistance de logiciels d'analyse vidéo, 10 000 heures d'images dans le cadre de l'instruction.
- A l'occasion de la disparition de la jeune Lina, le 23 septembre 2023, les enquêteurs ont dû exploiter manuellement plus de 2 To de données issues de 20 caméras de vidéoprotection, soit plus de 350 heures de visionnage. 3 enquêteurs y ont été affectés pendant 3 jours, puis un personnel pendant 7 semaines.
- A la suite des émeutes urbaines de juin 2023, les enquêteurs de la gendarmerie nationale ont récupéré, sur réquisitions, plus de 246 To de données dans une commune, soit environ 26 000 heures de visionnage et d'analyse (plus de 1 000 jours).
- Dans un dossier de pédo-pornographie, une enquête en cours nécessite l'analyse de 70 To de données retrouvées sur une cinquantaine de supports différents au domicile de plusieurs mis en cause, soit plus de 12 000 heures d'images.

En second lieu, la preuve numérique se généralise, y compris dans la délinquance du quotidien. Elle s'impose comme élément incontournable d'établissement de la conviction du juge, y compris lors de la garde à vue, dans la mesure où elle peut objectiver, dans certains cas de manière définitive, des éléments de preuve. Sa recherche devient donc un objectif majeur de l'enquête.

Les exemples donnés ci-dessus mettent ainsi en lumière l'absolue nécessité pour les enquêteurs de disposer d'outils de rationalisation de l'analyse des scellés vidéos, et, indirectement mais par voie de conséquence, de leur temps de travail. Tel est l'apport des logiciels d'analyse vidéo, qui assistent l'enquêteur dans la réalisation d'un acte désormais indispensable à la manifestation de la vérité, permettant de travailler à charge comme à décharge, mais qui, s'il est accompli « manuellement », peut s'avérer si chronophage que son bilan coût/avantage peut dans certains cas apparaître négatif. L'enquêteur, assisté par un logiciel qui le libère de l'obligation de visualiser la totalité des images sous scellés – et qui est potentiellement plus efficace que lui, parce qu'hermétique à toute perte de concentration dans la visualisation des flux d'images[21] - peut se consacrer à des tâches à plus grande valeur ajoutée.

Ces constats font consensus. Bien identifiés, ils ont conduit depuis plusieurs années à des réflexions en vue du développement de solutions logicielles souveraines, puisque c'est bien l'absence de telles solutions qui a conduit les forces de sécurité, lorsque le besoin est devenu urgent (attentats de 2015) ou patent (affaire Maëlys[22]), à se tourner vers les produits du marché comme le logiciel *BriefCam*.

Rapidement, des réflexions se sont ainsi engagées pour développer des solutions logicielles produites par l'Etat. *Sigma*, lancé dès 2015, s'inscrit dans cette logique. Il s'agit alors d'un projet numérique décliné en deux versions : un logiciel « expert », permettant de traiter des volumes très importants de vidéos, destiné aux seules unités spécialisées, et une version destinée aux enquêteurs des services et unités de proximité, avec des capacités plus limitées. A cette solution, sera finalement préférée la recherche d'un produit plus polyvalent et collaboratif, écartant la construction duale du projet Sigma : *Système V*.

[21] Selon la délégation ministérielle aux partenariats, stratégies et innovations de sécurité (DPSIS) du ministère de l'Intérieur, à laquelle a succédé la DEPSA, des recherches scientifiques ont montré que les opérateurs ne parviennent généralement pas à détecter les incidents après 20 minutes de visualisation d'une séquence vidéo. D'autres recherches ont également révélé qu'après 12 minutes de visualisation continue, un opérateur est susceptible de manquer jusqu'à 45 % de l'activité à l'écran, et jusqu'à 95% après 22 minutes. (Assemblée Nationale Rapport d'information n°1089 *sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité* 12 avril 2023 p.61).

[22] Disparition d'une fillette de huit ans, lors d'une réception de mariage. Le suspect, Nordahl Lelandais, sera condamné à la réclusion criminelle à perpétuité pour meurtre précédé d'enlèvement.

En cours de développement depuis avril 2020, *Système V* est un traitement prévu pour les enquêteurs de la police et de la gendarmerie nationales, répondant, comme *Sigma* et plusieurs produits du marché, aux besoins opérationnels d'analyse rapide d'importants volumes d'images vidéo. Comme le logiciel *BriefCam*, il permet d'analyser et d'exploiter les sources vidéo afin d'en extraire les seules séquences susceptibles de concourir à la résolution des enquêtes.

Système V, contrairement à ce qui a été fait pour *BriefCam* (cf. 1.2.1.2), a vocation à être déployé dans l'ensemble des services et unités en charge d'une mission de police judiciaire, ouvrant ainsi, potentiellement, une utilisation bien plus large de cet outil, notamment pour les enquêtes relevant de la délinquance du quotidien. Le dispositif, pour des raisons de sécurité et de secret de l'enquête, n'est pas centralisé : l'application est installée sur un serveur dédié relié au réseau local du service. Les utilisateurs y ont accès depuis leur poste de travail après authentification. Ils n'ont donc accès qu'aux données produites localement par leur service, sous réserve des habilitations qui leur sont données par le chef de service. Aucun tiers ne peut accéder aux données et aucun export de celles-ci n'est possible.

Système V a fait l'objet, respectivement par la DGPN (le 20 juillet 2023) et par la DGGN (le 21 novembre 2023), d'engagements de conformité au 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* (cf. 2.1.2.2).

Il est en cours de test dans 7 unités et services, et n'a vocation à être généralisé, selon un échéancier pluriannuel, qu'à compter de l'été 2024.

L'*annexe 3* en précise les modalités et les fonctionnalités.

1.1.2 Les fondamentaux des outils numériques d'aide à l'exploitation des images par les enquêteurs

1.1.2.1 Points communs et variables

Les outils numériques d'aide à l'exploitation des images vidéo ont des caractéristiques communes et des variables.

Ils reposent tous sur l'intelligence artificielle (IA), utilisant pour la plupart une technologie d'*« apprentissage profond »* faisant apprendre à la machine au lieu de la programmer donc de la prédéterminer. Ils permettent l'indexation de séquences vidéo, en fonction de critères sélectionnés par l'utilisateur, écartant les images ne répondant pas à ces critères. Les algorithmes fondant ces logiciels sont donc essentiels à leurs performances, qui sont variables selon les applications.

Les logiciels d'analyse vidéo se différencient en revanche par la relative diversité des différentes fonctionnalités qu'ils proposent, plus au moins nombreuses, élaborées et efficaces selon les algorithmes développés : détection d'« objets » par reconnaissance de leur forme (voiture, vélo, camion, bus, silhouette, présence d'un sac ou d'un masque…), directions de mouvements, couleurs, comportements, objets abandonnés, similitudes, reconnaissance faciale, reconnaissance de plaque d'immatriculation… Ils peuvent aussi permettre des calculs de flux, à des fins statistiques notamment.

L'efficacité des logiciels d'analyse vidéo dépend bien sûr des performances des algorithmes utilisés, mais aussi, en amont de ceux-ci, de la qualité des images vidéos qui les alimentent, la recherche d'objets sur des vidéos enregistrées de nuit étant nécessairement moins efficace qu'avec une bonne luminosité.

1.1.2.2 Les caractéristiques propres du logiciel *BriefCam*

La société israélienne *BriefCam* a été fondée en 2007 pour répondre au besoin d'algorithmes capables de traiter rapidement de grandes quantités de données vidéo. Le logiciel a notamment été utilisé dans l'enquête sur l'attentat terroriste d'Anders Breivik à Oslo, en juillet 2011, dans celle sur l'attentat de Boston, en avril 2013, et son usage s'est répandu dans de nombreux pays, y compris dans l'Union européenne (cf. *annexe 4*: comparaison internationale de l'utilisation des logiciels d'analyse vidéo). Depuis 2018, *BriefCam* est détenue par la société multinationale Canon.

BriefCam propose trois solutions différentes de son logiciel.

La solution « REVIEW » permet de traiter, *a posteriori*, des flux vidéo à partir de critères prédéfinis par l'application, sur la base desquels se fait la recherche. L'utilisateur ne peut à aucun moment créer ses propres critères de recherche : il n'a à disposition que ceux proposés, « sur étagère », par le logiciel. Il ne peut créer, avec cette solution, aucune base de données spécifique alimentée par le logiciel. Il n'est connecté à aucune base de données extérieure, ne pouvant fonctionner qu'en « vase clos », puisqu'il est installé sur un ordinateur dédié.

« RESPOND », solution plus sophistiquée, outre les fonctionnalités de « REVIEW », permet de traiter des vidéos en temps réel et de déclencher des alertes selon des règles définies par l'utilisateur.

La solution « RESEARCH » permet enfin la réalisation de tableaux de bord et d'analyses statistiques, mais aussi de vérifier le respect par les personnes de normes définies (port du masque…), ou de retracer le parcours d'un individu sélectionné dans une zone donnée[23].

Les services de police et les unités de gendarmerie ne disposent, respectivement depuis 2015 et 2017, que de la solution « REVIEW ». Ils n'ont jamais envisagé l'acquisition de solutions de niveau supérieur, contrairement, sans doute à d'autres opérateurs ou collectivités territoriales[24], qui n'étaient pas dans le champ de la mission.

La solution *BriefCam* est, à la base, conçue pour détecter et horodater automatiquement tous les « objets » en mouvement dans une vidéo. Elle repose sur le dispositif breveté « Vidéo SYNOPSIS », qui distingue *BriefCam* de produits concurrents et qui permet la visualisation en quelques minutes de tous les « objets » en mouvement, qui ont pu se produire à des moments variés.

Photographie n°1

Extraits d'une vidéo Synopsis illustrant l'affichage simultané de personnes et véhicules ayant circulé sur un même secteur à des moments différents (horodatage)

Source : documentation BriefCam

[23] On trouvera en *annexe 5* la présentation par l'éditeur du logiciel de ces différentes solutions et de leurs caractéristiques.
[24] Cf. CE 21 décembre 2023, référé n° 489990.

Si l'enquêteur dispose d'informations sur la victime ou l'auteur soupçonné, il peut faire une recherche par critères, le cas échéant en croisant plusieurs critères (vêtement ou véhicule et couleur, silhouette et port de sac, de masque ou de couvre-chef, direction de déplacement …). Pour chaque réponse fournie par l'application, un horodatage apparaît sur une vignette, à partir de laquelle l'enquêteur peut accéder directement à la séquence vidéo correspondante.

Photographie n°2

Recherche de déplacements en vélo vers le sud ; recherche de personnes portant un sac.

Source : Documentation BriefCam

En cas de résultat correspondant à la recherche de l'enquêteur, les images brutes jugées pertinentes peuvent être extraites de la vidéo originale pour alimenter le rapport versé à la procédure.
Considéré comme performant par les utilisateurs, le logiciel *BriefCam* connaît cependant certaines limites techniques : une sensibilité marquée aux images de caméras motorisées, rotatives ou mobiles[25], dont le mouvement propre perturbe la détection du mouvement des « objets » ; le nombre limité de formats de vidéo acceptés, les formats dits « propriétaires », c'est-à-dire qui ne sont pas dans le domaine public, n'étant pas reconnus et nécessitant une opération préalable de conversion ; des limites de volumétrie des vidéos pouvant être injectées dans l'application ; un temps pouvant être significatif de traitement algorithmique initial de la vidéo.

1.1.2.3 Les modalités d'utilisation

L'utilisation en police judiciaire des logiciels d'analyse vidéo obéit enfin à trois caractéristiques communes.

- S'agissant de la temporalité d'utilisation, l'exploitation des vidéos avec les outils d'aide à l'analyse se fait toujours en temps différé. Aucune utilisation n'est effectuée en temps réel (cf. section 2.2.2.2).

- L'exploitation de vidéos dans l'enquête à l'aide de logiciels[26] nécessite dans tous les cas une réquisition judiciaire des images brutes, délivrée au propriétaire du système vidéo concerné

[25] Ces caméras sont de plus en plus souvent choisies pour la vidéoprotection sur voies publiques des collectivités locales.
[26] Elle est soumise au secret de l'enquête rappelé par l'article 11 du code de procédure pénale (*« Sauf dans le cas où la loi en dispose autrement et sans préjudice des droits de la défense, la procédure au cours de l'enquête et de l'instruction est secrète. Toute personne qui concourt à cette procédure est tenue au secret professionnel… »*).

(collectivité territoriale, pour des images de caméras de voie publique, opérateur de transport public, personne privée). Cette réquisition est placée sous le contrôle d'un magistrat[27].

- S'agissant de l'utilisation des résultats de la recherche, les logiciels d'analyse vidéo ne constituent qu'une simple aide à la décision. Dans les faits, si l'outil permet de trier rapidement d'importants flux vidéo, le rôle de l'enquêteur demeure incontournable. C'est lui qui définit les critères de recherche. C'est lui qui met en perspective, à charge comme à décharge, les résultats automatisés de la recherche avec les autres éléments dont il dispose dans le cadre de ses investigations (témoignages, données relevant de la police technique et scientifique, exploitation de la téléphonie etc.).

En droit, en tout état de cause, la décision humaine ne peut jamais s'effacer derrière le résultat d'un traitement automatisé (cf. 2.2.2.2).

1.1.2.4 La question des relations entre les enquêteurs et les polices municipales en matière d'exploitation des images vidéo

Comme on l'a indiqué, les caméras de voie publique sont, pour l'essentiel, sous maîtrise d'ouvrage des communes et, dans une moindre mesure, des intercommunalités, beaucoup disposant par ailleurs d'un centre de supervision urbaine (CSU) centralisant les images prises par ces caméras[28]. Certains CSU sont équipés, en complément, de logiciels d'analyse vidéo, appartenant à la collectivité concernée, permettant ou facilitant l'exploitation des flux vidéo (par exemple, pour la recherche d'éléments matérialisant le non-respect du code de la route, ou des règles de stationnement, ou d'arrêtés municipaux relatifs aux ordures ménagères). Selon l'organisme *Disclose*, plus d'une centaine de municipalités et intercommunalités disposeraient en particulier du logiciel *BriefCam*, ce que confirment, pour trois d'entre elles, de récentes décisions de justice[29]. Le recours à ce type de logiciel par des collectivités locales n'appelle, en soi, aucune contestation juridique, dès lors qu'il est utilisé dans le cadre de leurs compétences.

Lorsqu'un acte de délinquance est commis sur la voie publique, les fonctionnaires de la police nationale et les militaires de la gendarmerie ont pour premier réflexe de sélectionner les caméras[30] se trouvant à proximité du lieu de commission, qu'elles soient publiques ou privées. La pratique générale est de saisir dès que possible la totalité des supports vidéo disponibles pour éviter la disparition de preuves éventuelles, compte-tenu du délai parfois très bref de conservation des données (72 heures par exemple pour la gare SNCF de Toulouse-Matabiau).

Pour des raisons strictement pratiques, il arrive dans certains cas[31], afin d'éviter des déplacements inutiles[32] ou de stériles saisies de vidéos qui n'apporteraient aucun élément probant pour l'enquête (panne technique d'une caméra non signalée à l'enquêteur, conditions matérielles d'enregistrement défavorables etc.) que des enquêteurs demandent aux opérateurs municipaux du CSU de s'assurer que les vidéos ciblées comportent bien des éléments susceptibles de les intéresser. Ces opérateurs peuvent alors pré-visualiser, en temps différé, les images vidéo, soit manuellement, soit, le cas échéant, en utilisant leur propre logiciel d'exploitation.

---

[27] Si dans le cadre d'une enquête judiciaire en matière de criminalité organisée, des caméras sont installées en application de l'article 706-96 du code de procédure pénale au titre des techniques spéciales d'enquête relevant de l'article 706-95-11, il n'y a pas de saisie des vidéos, puisque le service enquêteur en est dépositaire. En revanche, l'installation des caméras est autorisée par un magistrat et l'exploitation de la vidéo est actée en procédure.

[28] Un déport des images du CSU est parfois organisé vers le centre des opérations des forces de sécurité intérieure, permettant à celles-ci d'accéder directement aux images du CSU. Des protocoles sont dans ce cas formalisés entre les parties prenantes. Ces déports permettent aux services de sécurité de l'Etat de visualiser en direct les images prises par les caméras, sans enregistrement.

[29] Il s'agit de Nice (TA Nice référé n°2305692 23 novembre 2023), de Roubaix (TA Lille référé n°2310103 29 novembre 2023) et de la communauté de communes Cœur Côte Fleurie (TA Caen n°2303004 22 novembre 2023 et CE 21 décembre 2023 déjà cité).

[30] Dont ils disposent de la cartographie, s'agissant des caméras de voie publique.

[31] Et en fonction du degré de confiance de la relation entre les forces de sécurité de l'Etat et la police municipale concernée.

[32] Les opérations de saisies sur réquisition judiciaire peuvent nécessiter des déplacements d'enquêteurs pour procéder à des opérations techniques de transfert des vidéos sur des supports qui seront placés sous scellés.

S'ils confirment à l'enquêteur que la vidéo est susceptible de contenir des éléments exploitables, celui-ci pourra procéder alors à la saisie des images, pour en assurer l'exploitation judiciaire qu'il est seul habilité à faire.

Cette démarche auprès d'opérateurs municipaux, préalable à une éventuelle saisie, a une visée pragmatique et répond à une logique d'efficacité. Elle n'est jamais systématique, mais elle correspond cependant à une certaine réalité de terrain, ce qui pourrait susciter certaines interrogations juridiques. La mission retient néanmoins de ses échanges sur ce point précis avec les services et unités qu'elle a rencontrés que, dès lors que l'enquête relève d'un certain niveau de criminalité ou de sensibilité, toute démarche préalable de « levée de doutes » est écartée par les enquêteurs, qui procèdent alors directement à la saisie des vidéos, sans solliciter les opérateurs municipaux.

1.2 *BriefCam* : un logiciel acquis pour faire face à d'importants besoins émergents, mais inégalement déployé

1.2.1 Des acquisitions et une diffusion limitées, sans coordination ni doctrine formalisées

1.2.1.1 Des acquisitions dépourvues de doctrine

Comme on l'a indiqué en section 1.1.1.2, les décisions d'acquisition du logiciel *BriefCam* prises par la police et la gendarmerie nationales résultent d'abord du besoin, révélé par des événements dramatiques ou des affaires emblématiques, d'exploiter à des fins judiciaires une masse considérable d'images vidéo, de réduire le temps nécessaire à leur visionnage par le recours à un outil numérique[33] et de rationaliser le travail des enquêteurs en privilégiant d'autres activités à plus forte valeur ajoutée.

Les attentats de 2015 ont, principalement pour la police, généré une masse considérable d'images vidéo de toutes origines, difficilement exploitables dans un contexte de course contre la montre pour identifier des auteurs. En 2017, l'affaire Maëlys, traitée par la gendarmerie, a requis la mise à disposition de 15 enquêteurs pendant 7 jours pour exploiter les images saisies. C'est à la suite de ces deux évènements que la recherche d'outils permettant l'accélération des lectures vidéo a été engagée, parallèlement à la mise à l'étude d'une solution souveraine.

L'équipement des deux forces a suivi un calendrier et des choix de déploiements différents, mais il a relevé d'une même volonté : doter les enquêteurs d'un outil de rationalisation de l'exploitation des images vidéo, ayant vocation à n'être utilisé que dans le cadre judiciaire. La très grande majorité des licences et matériels dédiés ont d'ailleurs été financés sur les fonds de concours de l'AGRASC et de la MILDECA, entités dirigées (pour l'AGRASC) ou intégrant (pour la MILDECA) des magistrats, ce qui conforte la vocation strictement judiciaire du logiciel.

Pionnière, la police nationale a engagé une dotation au fil de l'eau entre 2015 et 2021. Mais ses acquisitions se sont faites sans plan de déploiement décidé au niveau de la direction générale, au gré du choix des services selon leur connaissance de l'outil, et à des niveaux de décisions différents, centralisé (police judiciaire) ou déconcentré (sécurité publique, pour ses activités de police judiciaire).

[33] Cet outil assure le *derushage* des images (du terme anglais *rush*, qui désigne toutes les vidéos brutes faites pendant un tournage), technique qui consiste à retirer des images brutes les parties superflues, et à sélectionner les seules séquences pertinentes.

La police judiciaire équipe ainsi le service central interministériel d'assistance technique (SIAT) du logiciel *BriefCam* en 2017 et ses antennes territoriales en 2018 et 2019. La direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) de la préfecture de police de Paris acquiert le logiciel en 2016, tandis que la direction opérationnelle des services techniques et logistiques (DOSTL)[34] teste de son côté ce logiciel en 2019 et 2020 dans le cadre d'un contrat de partenariat public-privé de tests sur la vidéo intelligente avec la société IRIS. Aucune autre décision de déploiement n'a été prise par le préfet de police.

Les quelques acquisitions par la sécurité publique ont, quant à elle, surtout reposé sur des initiatives locales. C'est ainsi que des personnels de la direction départementale de la sécurité publique (DDSP) de Seine-et-Marne ont découvert *BriefCam* lors d'un salon MILIPOL, conduisant à une acquisition après un prêt pour test en 2015 par la société *M2M Factory*, distributeur de *BriefCam* en France. De même, un agent de la DDSP de Haute-Garonne, qui a découvert le logiciel dans les mêmes circonstances, s'est investi personnellement sur le sujet et a obtenu l'autorisation de sa hiérarchie directe pour l'acquisition du logiciel en 2017.

Le service national de police scientifique (SNPS) s'équipe en juin 2021 d'une version régulièrement mise à jour, la dernière en date étant de 2023, l'inspection générale de la police nationale (IGPN) étant également dotée de deux licences début 2021 par l'ex-STSI[2] sans aucune expression de besoins de sa part.

La mission évalue le budget police consacré aux achats du logiciel *BriefCam*, soit directement auprès du revendeur *M2M Factory*, soit auprès de l'UGAP par bons de commande, à environ 700 000 € au total, pour 32 licences, dont 28 sont en état de fonctionnement à la date du présent rapport. L'*annexe 6* recense les licences *BriefCam* acquises par la police nationale ainsi que les services affectataires.

Dans la gendarmerie nationale, la commande initiale, réalisée par l'administration centrale, a été passée en décembre 2017 auprès de *M2M Factory* par l'intermédiaire de l'UGAP, pour 587 000 €, permettant d'équiper 37 unités. Financées par le fonds de concours de l'AGRASC, ces acquisitions ont bénéficié au service central du renseignement criminel (SCRC), dès février 2018 et à 36 sections de recherches (SR), entre janvier et septembre de la même année. 2 licences supplémentaires seront acquises en 2019, portant le volume total des licences de la gendarmerie à 39[35]. 2 licences seront mises à jour en 2020 au profit de SR (sur fonds MILDECA), le SCRC effectuant la mise à jour de sa licence en juin 2023 (*annexe 7*).

Au bilan, l'absence de stratégie ministérielle raisonnée d'équipement des services, ainsi que le caractère non pérenne de la ressource budgétaire dédiée à cet équipement ont conduit à la création, en police comme en gendarmerie, d'un parc de logiciels *BriefCam* composé de versions hétérogènes, inégalement mises à jour. Ce schéma d'acquisition empirique et différencié entre forces, et même en leur sein, a sans doute contribué à l'absence de tout questionnement sur le statut juridique du logiciel dans la procédure judiciaire, comme on le verra en section 2.1.1.

1.2.1.2 Des logiques de diffusion propres aux directions métier

Si le déploiement du logiciel *BriefCam* n'a pas fait l'objet d'une planification nationale ni d'une doctrine formalisée, il a néanmoins obéi à des logiques de diffusion propres aux directions utilisatrices. Dans la police nationale, la direction centrale de la police judiciaire (DCPJ), la direction centrale de la sécurité publique (DCSP) [36] et la préfecture de police ont, plus ou moins sciemment et en tout cas de façon peu explicite, retenu l'idée de complémentarité opérationnelle.

[34] Devenue la direction de l'innovation, de la logistique et des technologies (DILT).
[35] Soit : 37 pour les SR ; 1 pour le SCRC ; 1 pour l'office central de lutte contre la délinquance itinérante.
[36] Les appellations et les rattachements de nombreux services, notamment judiciaires, de la police nationale ont été modifiés depuis la mise en œuvre de la réforme territoriale de 2023. Par souci de clarté, cependant, les appellations et rattachements en vigueur au moment des acquisitions du logiciel BriefCam ont été conservées dans le présent rapport.

Ainsi, la DCPJ, plutôt que déployer au plus près des enquêteurs un logiciel coûteux et exigeant en ressources informatiques (ordinateur dédié, système d'exploitation et capacités GPU[37] importantes), a choisi d'équiper en priorité ses services d'appui technique, d'abord le SIAT central, dès 2017, puis ses antennes territoriales au fur et à mesure de leur création[38]. Ces services, d'assistance comme leur nom l'indique, ne procèdent pas eux-mêmes à des investigations mais agissent à la demande des services centraux de la DCPJ ou des services d'investigation territoriaux, pour mettre en œuvre des techniques spéciales d'enquêtes indispensables à la manifestation de la vérité. Au sein de la DCPJ, les services affectataires du logiciel *BriefCam* sont donc des prestataires de services, leur mission étant principalement d'assister les enquêteurs en leur fournissant un matériel adapté à leurs besoins et en les soulageant de certaines tâches nécessitant une compétence technique particulière.

La DCSP a suivi une logique de déploiement similaire. Les logiciels qu'elle a financés, exclusivement dédiés aux services à vocation judiciaire de cette direction, ont été prioritairement installés dans des sûretés départementales (SD). Echelon le plus spécialisé de l'activité judiciaire au sein des directions départementales de la sécurité publique (DDSP)[39], les SD ont, dans le domaine judiciaire, un rôle d'assistance et de renforcement des circonscriptions de sécurité publique, d'impulsion et d'animation de la lutte contre la criminalité et de coordination des moyens techniques relevant de la sécurité publique. Leur importance explique le rôle précurseur joué par certaines d'entre elles dans l'acquisition du logiciel *BriefCam*, ainsi que leur fréquence d'utilisation de ce logiciel, relativement élevée (cf. infra), soit au bénéfice des différents groupes qui les constituent, soit, dans cette logique d'assistance, au profit des enquêteurs de terrain.

La logique de déploiement a, *de facto*, été la même à la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) de la préfecture de police : l'unique logiciel *BriefCam* acquis par la préfecture a été attribué à l'unité d'appui technique (UAT), qui utilise cet équipement en appui des services judiciaires de la DSPAP (pour le reformatage des vidéos saisies par les enquêteurs après réquisition, l'assistance au processus de « derushage » etc.).

En ce qui concerne la gendarmerie nationale, les principes de déploiement semblent plutôt s'attacher au niveau de criminalité traité par les unités, sans négliger cette logique d'assistance aux enquêteurs. Les 39 licences du logiciel *Briefcam* ont été attribuées aux unités de police judiciaire dites du « haut du spectre » que représentent les SR et un office central, mais également, dans cet esprit d'assistance technique aux enquêteurs, le SCRC.

Concernant le déploiement du logiciel, on relèvera une singularité au sein de la police nationale, liée au fait que certaines directions ont financé l'achat de logiciels qui ont été utilisés par des services relevant d'autres directions. C'est le cas de la DCSP, qui a financé l'achat de licences, certes pour la SD du Rhône, mais avec une installation dans l'antenne SIAT de Lyon, relevant de la DCPJ, où il a été exploité jusqu'en 2022. Il en va de même du logiciel utilisé par la police judiciaire de Nice, acquis sur le budget DCSP pour la SD des Alpes-Maritimes.

1.2.2 Un logiciel utile et performant, mais sous-utilisé

Tous les utilisateurs rencontrés soulignent l'utilité du logiciel *BriefCam*, perçu comme un outil performant, permettant un gain de temps remarquable dans l'exploitation des sources vidéos. Des utilisateurs indiquent même qu'à défaut d'un tel logiciel, ils renonceraient, dans les affaires les moins graves, à une exploitation systématique des sources vidéo disponibles, donc à un moyen de preuve particulièrement efficace.

[37] Le GPU (Graphics Processing Unit) est un processeur graphique.
[38] Ces antennes sont installées au sein des directions interdépartementales de police judiciaire (DIPJ) de Marseille, Lyon, Bordeaux, Lille, Strasbourg, Rennes, Antilles-Guyane et de la direction régionale de la police judiciaire (DRPJ) de Versailles.
[39] Leurs missions sont définies par la circulaire DGPN 95-17088 du 27 novembre 1995. Elles sont chargées de lutter contre toutes les formes de délinquance de voie publique, la toxicomanie et le trafic de drogues locaux, contre l'immigration irrégulière et les violences urbaines. Elles peuvent également comporter des services de protection des mineurs ou de protection de la famille.

L'étude des données d'utilisation du logiciel dont la mission a pu disposer fait néanmoins apparaître une sous-utilisation du logiciel, pouvant, en première analyse, interroger sur le retour sur investissement.

1.2.2.1 Le constat de la sous-utilisation

La mission fait d'abord le constat qu'il n'existe aucun enregistrement systématique et continu par les services, permettant d'avoir une vision complète des utilisations de *BriefCam* entre 2015 et 2023[40]. Le logiciel ne conserve de son côté aucune archive informatique des données exploitées après traitement. Comme on le verra en effet, les données du « journal d'audit », qui assure la traçabilité des utilisations, sont effacées après 365 jours. D'autre part, si l'on considère le logiciel *BriefCam* comme un logiciel de rapprochement judiciaire (LRJ) au sens de l'article 230-20 du code de procédure pénale (cf. 2.1), *« les données exploitées à caractère personnel éventuellement révélées par l'exploitation des* [LRJ] *sont effacées à la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans »*[41]. Même si la traçabilité informatique de *BriefCam* s'inscrivait dans la durée, elle serait donc neutralisée par les dispositions précitées du code de procédure pénale.

La mission doit donc se contenter de remontées déclaratives reposant pour l'essentiel sur la mémoire des utilisateurs.

Au bénéfice de cette remarque et avec la prudence qu'elle impose, on recense, dans la police nationale, 177 utilisations déclarées du logiciel entre 2015 et 2023, soit 8 utilisations par an en moyenne pour l'ensemble des services affectataires, et 5,5 utilisations par licence sur l'ensemble de la période. Trois services totalisent plus de 57 % des utilisations[42], l'un d'entre eux[43] comptant à lui seul 31 % des utilisations.

Dans la gendarmerie nationale, 386 utilisations ont été déclarées, ce chiffre correspondant toutefois aux deux seules dernières années (2023 et 2022).

La fréquence d'utilisation est très contrastée.

[40] L'absence d'enregistrements systématiques des utilisations peut résulter du fait que les utilisateurs étaient, pour la plupart, en même temps administrateurs du logiciel, fournissant le plus souvent, à ce titre, quelques prestations d'assistance aux enquêteurs, dont ils n'ont pas estimé nécessaire de conserver des traces écrites. Cependant, dans les services où le recours au logiciel a été plus fréquent, comme à Toulouse ou Cergy, les administrateurs ont pu prendre l'initiative de créer un fichier récapitulatif des utilisations. Mais ces enregistrements ont été tardifs et sont donc incomplets.
[41] Article 230-22 du code de procédure pénale.
[42] Les SD de Toulouse, de Cergy et la DSPAP.
[43] Le SD de Toulouse.

Encadré n°2 : fréquences d'utilisation du logiciel *BriefCam*

Dans la police nationale, sur les 18 services attributaires de *BriefCam :*

* 7 déclarent l'avoir utilisé entre 0 et 1 fois

* 5 déclarent l'avoir utilisé entre 2 et 10 fois

* 3 déclarent l'avoir utilisé entre 11 et 20 fois

* 2 déclarent l'avoir utilisé entre 21 et 25 fois

* 1 déclare l'avoir utilisé 55 fois

Dans la gendarmerie nationale, sur les 39 unités utilisatrices de *BriefCam* :

* 4 déclarent l'avoir utilisé entre 0 et 1 fois

* 26 déclarent l'avoir utilisé entre 2 et 10 fois

* 6 déclarent l'avoir utilisé entre 11 et 20 fois

* 1 déclare l'avoir utilisé entre 21 et 25 fois

* 2 déclarent l'avoir utilisé entre 26 et 50 fois

La sous-utilisation du seul logiciel d'analyse vidéo attribué aux services est donc patente, contrastant avec le constat de son efficacité fait par les enquêteurs, qui tous l'estiment indispensable dans un contexte d'augmentation massive et continue des données numériques dans les enquêtes judiciaires. Plusieurs raisons expliquent ce paradoxe.

1.2.2.2 Les raisons de la sous-utilisation

Tout d'abord, le logiciel *BriefCam* est mal connu des enquêteurs de terrain, du fait de l'absence de toute information institutionnelle sur son existence, sa disponibilité et ses fonctionnalités. Le déploiement vers les seules unités spécialisées prestataires de services aurait dû s'accompagner d'une information spécifique et structurée des enquêteurs, qui a totalement fait défaut (de la part des directions métier) ou qui a été très marginale (lors de réunions entre les SIAT ou les SD et les services d'enquête locaux). *Briefcam* est ainsi resté confidentiel, le plus souvent cantonné aux services affectataires, et lorsqu'il a été employé par certains enquêteurs, c'était le plus souvent à la faveur d'un rapport de proximité ou au bénéfice de relations personnelles avec le service affectataire.

Ensuite, aucun dispositif de formation des utilisateurs n'a été prévu. Certes relativement intuitif, *BriefCam* nécessite néanmoins une formation-utilisateurs que n'offrait pas, de son côté, le distributeur du logiciel. La formation s'est donc faite le plus souvent sur le « tas »[44].

Enfin, d'autres obstacles ont entravé une utilisation généralisée du logiciel. Ainsi, la nécessité pour l'enquêteur, faute d'une solution de télé-versement sécurisée, de se déplacer dans le service affectataire pour y déposer ses sources vidéos est évidemment pénalisante, surtout pour les services géographiquement éloignés. De même, les limites techniques du logiciel *BriefCam*, dont il a été question en section 1.1.2.2 ont également pu constituer un frein à son utilisation. De même encore, compte tenu du coût des mises à jour et des remplacements de matériels, l'absence de continuité du suivi budgétaire a pu démotiver des services à utiliser un logiciel devenu moins performant.

Le constat doit donc être fait que, d'un point de vue quantitatif, l'utilisation effective du logiciel *BriefCam* par les forces de sécurité intérieures (FSI) a été très marginale, contrairement à ce qu'a pu laisser entendre une certaine presse.

[44] Une bonne pratique a cependant été relevée au sein de l'IGPN, qui met à disposition de ses enquêteurs, sur son site intranet, des tutoriels élaborés par son service informatique permettant une auto-formation. En gendarmerie, des administrateurs ont également conçu des tutoriels au bénéfice des utilisateurs.

La mission considère néanmoins que l'appréciation de l'efficience d'un tel logiciel ne peut se résoudre à une équation comptable entre son coût d'acquisition et le nombre de ses utilisations. Elle doit d'abord être évaluée au regard de sa pertinence intrinsèque dans la mission de police judiciaire, pour l'élucidation des délits et des crimes et le service rendu aux victimes. À cet égard, il est indéniable que le logiciel a contribué à la résolution de plusieurs affaires judiciaires, dont certaines graves et médiatisées, ayant entraîné des préjudices importants, ce qui suffit à établir sa légitimité.

2 L'IDENTIFICATION TARDIVE DU CADRE JURIDIQUE D'UTILISATION DES LOGICIELS D'ANALYSE VIDEO ET LE FAUX PROBLEME DE LA RECONNAISSANCE FACIALE

2.1 L'identification du cadre juridique d'utilisation des logiciels d'analyse vidéo : un processus très lent

2.1.1 La question du statut juridique du logiciel a été négligée

Tant dans la police que dans la gendarmerie, les acquisitions de *BriefCam* ont été réalisées sans évaluation juridique, que ce soit au niveau local ou central. Cette absence de questionnement initial sur le cadre d'utilisation d'un logiciel d'analyse vidéo peut s'expliquer par diverses raisons.

2.1.1.1 Les raisons de l'absence d'interrogation sur le statut juridique du logiciel

Premièrement, contrairement à un produit souverain (logiciel, système d'information…), dont la conception s'inscrit nécessairement dans une certaine durée et qui, de ce fait, passe par des phases d'évaluations techniques, mais aussi, dès l'origine, de définition de son cadre légal, un produit « sur étagère » acheté sur le marché, surtout sans recensement de besoins pluriannuels (comme cela s'est produit pour *BriefCam*, acheté, comme on l'a vu, en mobilisant prioritairement des fonds de concours), échappe plus facilement aux interrogations juridiques concernant son statut.

En deuxième lieu, les achats de licences *BriefCam* par les FSI sont intervenus entre 2016 et 2019[45]. Les évolutions juridiques découlant de la directive 2016/680 *« police-justice »* du 27 avril 2016[46] ont quant à elles été transposées dans la loi « informatique et libertés » du 6 janvier 1978[47] avec une entrée en vigueur le 1er juin 2019, soit après la plupart de ces achats, et les services de l'Etat ont eu besoin d'un temps d'acculturation avant de s'interroger sur l'application des nouvelles règles européennes aux traitements de données existants.

Troisièmement, son achat était validé par la hiérarchie, le logiciel étant même le plus souvent fourni d'initiative par les directions centrales, comme dans le cas des SR de la gendarmerie nationale ou des SIAT de la police judiciaire. Cette « onction » hiérarchique ôtait légitimement tout doute des enquêteurs sur la licéité de son utilisation en procédure. De plus, jusqu'en novembre 2018, le logiciel ne comportait aucune fonctionnalité de reconnaissance faciale[48], pouvant potentiellement questionner son statut juridique.

Enfin, *BriefCam* a été appréhendé par les enquêteurs de terrain comme un « super magnétoscope » ou une « grosse loupe », permettant essentiellement de repérer très rapidement les « objets » en mouvement passant dans le champ de la caméra. De bonne foi, les utilisateurs ne l'ont donc pas considéré comme pouvant avoir un statut spécifique dans la procédure, d'autant qu'il a toujours été installé sur un ordinateur dédié, déconnecté de toute base de données. Surtout, contrairement

[45] A l'exception des licences de l'inspection générale de la police nationale (IGPN) et du service national de police scientifique (SNPS), 3 au total achetées en 2021, et de la licence de la direction territoriale de la police nationale (DTPN) de la Guadeloupe, en 2023.
[46] Directive (UE) 2016/680 du Parlement et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[47] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[48] Comme on l'a indiqué, la fonctionnalité de reconnaissance faciale apparaît sur la version 5.3 commercialisée à compter de novembre 2018.

à certains LRJ[49], *BriefCam* ne produit aucune pièce ni documentation pouvant intégrer la procédure : il se limite à la réduction, par l'utilisation de critères prédéterminés choisis par l'enquêteur, du nombre d'images utiles à l'enquête et du temps de leur visualisation.

De ce fait, *Briefcam* n'a pas été perçu par les services enquêteurs, pourtant très attentifs au respect du droit puisqu'il en va du sort de la procédure qu'ils conduisent, comme un LRJ au sens du décret n°2012-687 du 7 mai 2012.

Au niveau de l'administration centrale, le faible nombre de licences acquises par les services de l'Etat[50] a fait de *Briefcam*, et plus globalement des logiciels d'analyse vidéo à des fins judiciaires, un sujet marginal au regard des problématiques juridiques lourdes posées par les très nombreux autres traitements de données utilisés par les forces de sécurité intérieure (FSI), plus sensibles en matière de libertés publiques (traitement des antécédents judiciaires (TAJ) ; fichier national des empreintes génétiques (FNAEG) ; automatisation de la consultation centralisée de renseignements et de données (ACCReD) ; fichier des personnes recherchées (FPR), etc.), devant être rendus compatibles avec le *« paquet européen de protection des données à caractère personnel »* issu du règlement général de protection des données (RGPD) et de la directive « police-justice ».

Jusqu'à une date récente, sur laquelle on reviendra, *BriefCam* n'a donc soulevé aucune question de statut juridique pour les services enquêteurs.

2.1.1.2 Les effets en procédure

Briefcam n'étant pas déclaré comme LRJ pour les raisons qui viennent d'être présentées, son utilisation n'a jamais été mentionnée dans les procédures judiciaires où il a été mis en oeuvre depuis son acquisition, dans lesquelles il n'a jamais donné lieu à demande d'autorisation du magistrat prévue à l'article R.40-40 du code de procédure pénale[51]. Le logiciel ne produisant pas de rapports ni de pièces spécifiques, les enquêteurs ont au demeurant versé en procédure, non pas les images re-traitées par *Briefcam* (vignettes horodatées), mais les images brutes extraites des vidéos originales, sélectionnées par eux et annexées à un procès-verbal d'exploitation des vidéos qui, lui, est versé à la procédure.

On signalera par ailleurs que la pratique de l'autorité judiciaire semble être de délivrer aux services enquêteurs, sur la base de l'article 230-20 du code de procédure pénale, des autorisations d'utiliser « les » LRJ, formulation générale qui évite une désignation nominative des différents logiciels réglementairement autorisés[52].

[49] Par exemple, dans la police nationale, ASTERIA (Analyse Simplifiée et Traitement des Eléments Recueillis par Intelligence Augmentée), dédié à la lutte anti-terroriste, permet une analyse des données extraites des supports d'une même procédure, en les classant, les organisant et les présentant sous forme intelligible pour l'enquêteur, qui peut alors interroger la base de données ainsi constituée de requêtes adaptées à ses besoins. ASTERIA produit donc une base de données qui lui est propre. De la même façon, le logiciel MERCURE permet, dans le cadre des interceptions judiciaires, l'exploitation automatisée des données de téléphonie et permet d'en extraire des synthèses. Dans la gendarmerie nationale, le logiciel ANACRIM (constitué de quatre logiciels de rapprochement judiciaire) permet, par exemple, de croiser des relevés bancaires et des données de téléphonie, recueillis sur réquisition judiciaire, ou de produire, à partir de données de procédure, des graphes relationnels ou évènementiels pour représenter, par exemple, des réseaux de relations entre différentes entités ou des individus. L'application DA-TD permet quant à elle de mettre en évidence des relations interpersonnelles (principaux correspondants) et la localisation géographique de personnes à partir d'investigations téléphoniques

[50] Pour mémoire (cf. 1.2.1.1), 32 licences ont progressivement été achetées par des services de la police nationale entre 2016 et 2023 ; 39 entre 2017 et 2019 pour des unités de la gendarmerie nationale

[51] *« La mise en œuvre des logiciels de rapprochement judiciaire mentionnés aux articles 230-20 et suivants est autorisée, pour chaque procédure qu'il contrôle, par le magistrat saisi de l'enquête ou chargé de l'instruction. En matière d'enquête de flagrance, l'autorisation est réputée acquise sauf décision contraire du procureur de la République »*

[52] Dans les procédures où *BriefCam* a été utilisé et où, par ailleurs, le recours aux LRJ a été sollicité par le service enquêteur et autorisé par le magistrat, cette désignation générique pourrait donc possiblement régulariser le recours à un outil d'analyse vidéo qui n'était pas encore déclaré comme LRJ, si la procédure venait à être contestée. Cette dernière hypothèse paraît au demeurant improbable puisque, précisément, l'utilisation du logiciel n'apparaît pas dans les pièces de procédure.

2.1.2 La prudente mais tardive qualification de logiciel de rapprochement judiciaire

Le logiciel *BriefCam* n'ayant été compris que comme un outil d'accélération du temps d'exploitation des vidéos, il a échappé, pendant près de 8 ans, à la détermination et l'officialisation, par les services du ministère de l'intérieur, du cadre juridique de son emploi par les forces de sécurité. Des hésitations d'analyse juridique doublées d'une certaine inertie administrative peuvent l'expliquer. Etonnamment, une fois l'expertise juridique assurée et assumée, la police et la gendarmerie nationales ont suivi deux stratégies différentes de « régularisation ».

2.1.2.1 La longue détermination du cadre juridique d'emploi du logiciel d'analyse vidéo *BriefCam*

Si un questionnement sur le statut du logiciel *BriefCam* est apparu assez rapidement à l'initiative de la DGPN et de la préfecture de police, l'analyse juridique a connu quelques errements.

Dès le 13 février 2017, la DGPN avait saisi la direction des libertés publiques et des affaires juridiques (DLPAJ), il est vrai sans citer le logiciel *BriefCam*, d'un projet de décret en Conseil d'Etat après avis de la CNIL, autorisant des traitements de données personnelles permettant l'analyse des enregistrements vidéo dans le cadre d'enquêtes judiciaires. Cette saisine se référait au II de l'article 26 de la loi du 6 janvier 1978, dans sa rédaction alors en vigueur, sans renvoi à la catégorie juridique des LRJ. Elle n'a pas eu, alors, de réponse.

Par note du 22 mars 2019, en revanche, en réponse à une sollicitation de la préfecture de police sur le cadre juridique d'expérimentation du logiciel *BriefCam*, la DLPAJ examinait le statut de ce logiciel par rapport à la seule loi « informatique et libertés », en l'analysant comme un traitement de données à caractère personnel, et non comme un LRJ relevant de l'article 230-20 du code de procédure pénale.

Or cet article définit les LRJ comme ceux *« destinés à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires »* qui sont réunies par les services de police judiciaire au cours de leurs investigations.

Une interprétation restrictive de cette définition pourrait supposer un « croisement » de données, qui matérialiserait le *« rapprochement d'informations »* évoqué par cet article. Or, comme on l'a vu, *BriefCam*, comme, demain, la solution souveraine *Système V*, ne croise pas de données et ne produit aucune documentation qui lui serait propre (graphes, bases de données nouvelle, synthèses etc.)[53].

Mais, au bénéfice d'une interprétation plus ouverte de l'article 230-20 du code de procédure pénale, on peut à l'inverse qualifier les logiciels d'analyse vidéo en général, *BriefCam* en particulier, de LRJ. La recherche automatisée à laquelle ils procèdent d'éléments pouvant contribuer à la manifestation de la vérité, qui seront ensuite versés à l'enquête, peut en effet caractériser un LRJ, dans la mesure où elle facilite *« l'exploitation et le rapprochement d'informations sur les modes opératoires »* des auteurs d'infractions, au sens de cet article. Les systèmes de vidéo-protection constituent des *« traitements de données personnelles »*[54]. Les logiciels d'analyse vidéo sont donc, à ce titre, dans le champ d'application de l'article 1er du 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*.

C'est cette interprétation qui a été faite par le ministère de l'intérieur, au terme de 8 années d'utilisation flottante au plan juridique. Il en résulte désormais en procédure, trois importantes conséquences qu'énonce l'article R. 40-40 du code de procédure pénale : la mise en œuvre du logiciel d'analyse vidéo doit être autorisée, pour chaque procédure qu'il contrôle, par un magistrat. Cette mise en œuvre ainsi que l'autorisation de l'autorité judiciaire doivent faire l'objet d'une

[53] Cet état de fait neutralise par conséquent le dernier alinéa de l'article R. 40-40 du code de procédure pénale, qui prévoit la jonction au rapport prévu par cet article *« de l'ensemble des données et informations exploitées »*, ce qui fait référence à des éléments de procédures extrinsèques, et non à images vidéo brutes, seulement « sélectionnées » par le logiciel.
[54] En application de l'article L. 251-1 CSI.

mention en procédure. A la clôture de l'enquête, l'exploitation des données ainsi rapprochées doit donner lieu à l'établissement d'un rapport joint à la procédure.

Au-delà de la question juridique, cette qualification de *BriefCam* comme LRJ présente une opportune utilité « d'affichage » : l'article 230-26 du code de procédure pénale prohibant toute utilisation à des fins administratives des LRJ, cette qualification conforte juridiquement l'absence de fait, constatée par la mission, de toute exploitation en temps réel, à des fins administratives, par les services attributaires.

2.1.2.2 Une qualification juridique qui se traduit par des stratégies différentes de clarification

C'est donc, au final, cette laborieuse analyse juridique qui a conduit le ministère de l'intérieur à ranger au nombre des LRJ les logiciels d'analyse vidéo mis à la disposition de ses services de police judiciaire (*BriefCam*) ou qu'ils vont utiliser dans l'avenir (*Système V*).

Selon l'article 6 du décret du 7 mai 2012, la mise en œuvre de tels logiciels *« s'accompagne »* de l'envoi à la CNIL d'un engagement de conformité, désormais doublé, depuis le 22 juin 2018, date d'entrée en vigueur de la loi du 21 juin 2018[55], d'une analyse d'impact sur la protection des données (AIPD), dès lors que ces traitements sont, par nature, susceptibles d'engendrer un risque élevé pour les droits et libertés.

La DGPN a par conséquent déposé le 14 décembre 2023 auprès de la CNIL un engagement de conformité au décret du 7 mai 2012 du logiciel *BriefCam*. La CNIL en a accusé réception le 15 décembre, après avoir fait de même, le 20 juillet de la même année, toujours pour la DGPN, pour le logiciel comparable *Système V*, destiné à remplacer *BriefCam* et disposant de fonctionnalités équivalentes, à l'exception de la reconnaissance faciale et de la reconnaissance de plaques. Dans l'attente des conclusions du présent rapport, instruction a été donnée aux services de police judiciaire de suspendre l'utilisation du logiciel *BriefCam*.

Quant à la DGGN, si elle a également déposé un engagement de conformité de *Système V* auprès de la CNIL dont il a été accusé réception le 21 novembre 2023, elle s'est en revanche abstenue de faire de même pour *BriefCam*, après avoir également donné instruction à toutes ses unités et services, le 17 novembre 2023, de « suspendre » l'utilisation de *BriefCam « pour des raisons d'insécurité juridique »*.

On constate ainsi une différence de méthode entre la police et la gendarmerie nationales quant au dépôt auprès de la CNIL d'un engagement de conformité du logiciel *BriefCam*, sur laquelle on reviendra en partie 3.

2.2 La reconnaissance faciale dans l'analyse vidéo par la police et la gendarmerie nationales : du fantasme aux réalités

La reconnaissance faciale est très strictement encadrée en droit français. Dès lors qu'elle repose sur une technique biométrique[56], donc sur une donnée dite « sensible », elle est par principe prohibée par l'article 6 de la loi « informatique et libertés », sauf pour *« les traitements* (…) *justifiés par l'intérêt public ».*

[55] Loi n° 2018-493 du 20 juin 2018 *relative à la protection des données personnelles*, qui transpose la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des 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 et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[56] Selon la CNIL, *« la reconnaissance faciale est une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier. La reconnaissance faciale appartient à la catégorie plus large des techniques biométriques ».* Ces techniques *« permettent ou confirment l'identification unique des personnes ».* « Reconnaissance faciale : pour un débat à la hauteur des enjeux » 15 novembre 2019, p.3.

En police administrative, son utilisation en temps réel dans l'espace public est interdite[57]. La loi du 19 mai 2023 sur les jeux olympiques et paralympiques[58] ne fait pas exception. Elle innove certes en autorisant pour la première fois, à titre expérimental, la mise en œuvre en temps réel de traitements algorithmiques d'images de vidéoprotection, en procédant à *« un signalement des situations d'attention »* pour les forces de l'ordre[59]. Mais le IV de son article 10 précise que ces traitements algorithmiques *« n'utilisent aucune donnée biométrique et ne mettent en cause aucune technique de reconnaissance faciale »*.

L'article 88 de la loi de 1978[60], pris pour la transposition de la directive « police-justice » autorise en revanche certaines utilisations de techniques biométriques, dont la reconnaissance faciale, en police judiciaire, laquelle a pour finalité la recherche des auteurs d'infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, ce qui correspond à une *« nécessité absolue »* au sens de cette loi[61]. Le décret en Conseil d'État pris après avis de la CNIL autorisant le TAJ[62], qui comporte plusieurs millions de photographies de personnes mises en cause ou disparues, en est à ce jour, en police judiciaire, l'unique illustration.

Pourtant, Disclose faisait état, dans l'article déjà évoqué et sans en préciser le cadre (judiciaire ou administratif), de l'utilisation par des services de la police nationale du logiciel *BriefCam*, qui *« permet de traquer une personne sur un réseau de caméras grâce, par exemple, à la couleur de son pull (…)* [de] *suivre un véhicule à l'aide de sa plaque d'immatriculation ou* [d'] *analyser des visages »*, dénonçant ainsi une utilisation illégale de la reconnaissance faciale.

2.2.1 Réalités de la reconnaissance faciale dans le logiciel *BriefCam*

Cet organisme laisse ainsi entendre que des policiers utiliseraient *BriefCam* en temps réel, et non pas en temps différé, et qu'ils auraient un large recours à la technologie de la reconnaissance faciale.

2.2.1.1 Recherche par similarité et reconnaissance faciale

La technologie initiale développée par *Briefcam* est celle de la recherche par similarité**.** Elle ne s'appuie pas sur des vecteurs ou données mathématiques, biométriques notamment, et ne crée pas de "gabarits" susceptibles de constituer des bases de données[63]. La recherche par similarité repose alors sur l'analyse des pixels créés par les images, permettant de discriminer les "objets" en mouvement passant dans le champ de la caméra : véhicules, personnes, animaux, etc.

Au fil des versions[64], l'éditeur a fait évoluer le produit en affinant les critères de filtre : sexe (homme/femme), taille (adulte/enfant), catégorie de véhicule (vélo, moto, camion, voiture…), animaux, attributs des personnes (vêtement, visage masqué, couvre-chef, sac…), vitesse, direction, couleur, similitude d'apparence, etc. Il a, sur la base de la même technologie, ajouté la "similitude

[57] Sauf si elle est activée par la personne elle-même, qui, volontairement, accepte son authentification biométrique. C'est le cas avec le traitement PARAFE pour le passage des frontières.
[58] Loi n° 2023-380 relative aux jeux olympiques et paralympiques 2024 et portant diverses autres dispositions.
[59] Cette loi autorise plus précisément la mise en œuvre de traitements algorithmiques pour détecter en temps réel des évènements prédéterminés (dont la nature est précisée par le décret n°2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 relative aux jeux olympiques et paralympiques 2024) susceptibles de présenter ou révéler des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes.
[60] *« Le traitement de données mentionnées au I de l'article 6 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, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée »*
[61] Conseil d'État *Association La Quadrature du Net* 26 avril 2022 n° 442364.
[62] Décret n°2012-652 du 4 mai 2012 *relatif au traitement d'antécédents judiciaires*, codifié aux art. R40-23 et suiv. du code de procédure pénale.
[63] Tel est le cas, en revanche, de technologies s'appuyant sur des *hash perceptuels*, ou d'analyses en composantes principales, auxquelles recourt Google Image Search par exemple.
[64] Une cinquantaine depuis la commercialisation de *BriefCam* en 2013.

de visages" qui permet d'afficher tous les objets assimilés à des "visages" passés dans le champ de la caméra, et, en mars 2020, dans la version 5.6, un filtre alphanumérique intitulé "reconnaissance de plaques", qui permet de rechercher des séries de chiffres et lettres, ou de rechercher une suite alphanumérique particulière[65].

En novembre 2018, l'éditeur a introduit dans une nouvelle mise à jour (version 5.3), une fonctionnalité intitulée "reconnaissance faciale" sans informer particulièrement les utilisateurs du produit. Elle permet d'injecter dans le logiciel une ou plusieurs photos extérieures afin de les comparer aux visages présents dans les vidéos exploitées par *BriefCam*, constituant ainsi une base de données. L'éditeur indique qu'en termes de capacités, le logiciel peut recevoir jusqu'à 500 photos.

Selon les informations communiquées à la mission par l'éditeur et confirmée par le « livre blanc » du logiciel, la fonctionnalité de reconnaissance faciale utilise une technologie biométrique, puisqu'elle constitue des « identifiants uniques » de visage[66], ce qu'avait déjà relevé la presse spécialisée américaine dès 2018.

Evidemment, la précision de la reconnaissance faciale dépend fortement de la qualité de la vidéo et de celle de la photo injectée. Après comparaison, chaque image se voit en conséquence attribuer 1, 2 ou 3 étoiles par le logiciel. En général, 1 étoile correspond aux visages dont *BriefCam* ne peut pas extraire les caractéristiques biométriques et les comparer à d'autres visages, 2 étoiles correspondent aux visages dont *BriefCam* peut extraire ces caractéristiques avec une confiance moyenne, 3 étoiles correspondant à une confiance élevée.

Enfin, la société a précisé à la mission que le logiciel ne stockait aucune donnée sur le disque dur, à l'exception du « journal d'audit » évoqué au 1.2.2.1. Les vecteurs mathématiques utilisés pour la comparaison faciale sont donc supprimés en même temps que les vidéos au terme de l'exploitation.

2.2.1.2 Le risque juridique de l'existence d'une fonctionnalité de "reconnaissance faciale" dans le logiciel *Briefcam* a été très limité dans les faits par les conditions d'utilisation

Comme on l'a rappelé ci-dessus, l'utilisation de la reconnaissance faciale est aujourd'hui strictement encadrée en droit français, tant en police administrative qu'en police judiciaire. La mise à disposition des services, à compter de novembre 2018, d'une version de *BriefCam* comportant une fonctionnalité de reconnaissance faciale pouvait donc constituer une source de vulnérabilité juridique pour les utilisateurs du logiciel, d'autant plus que cette fonctionnalité devenait présente par défaut, ne pouvant être désactivée qu'après une intervention informatique de l'administrateur (le gestionnaire/utilisateur du logiciel désigné par la hiérarchie du service).

Dans les faits, cette vulnérabilité juridique a cependant été quasiment neutralisée par plusieurs réalités objectives :

- comme on l'a indiqué, toutes les licences achetées par les services ne disposaient pas, compte tenu de l'absence de suivi des mises à jour, de cette fonctionnalité. Pour l'ensemble des services, 29 licences comprennent aujourd'hui la fonctionnalité de reconnaissance faciale, soit 43% du parc de logiciels *BriefCam*. Lorsqu'elles en disposaient, elles n'étaient pas toutes exploitées sur du matériel susceptible de la faire fonctionner (nécessité d'une carte GPU spécifique). ;

[65] Il ne s'agit pas d'une lecture automatisée des plaques d'immatriculation (LAPI), le logiciel restituant aussi bien une plaque d'immatriculation qu'un logo alphanumérique affiché sur l'arrière d'une camionnette et n'étant connecté à aucune base de données comme le système d'immatriculation des véhicules (SIV), le fichier des véhicules volés (FVV) ou le système d'information Schengen (SIS).

[66] Livre blanc *« Reconnaissance des visages »* de l'éditeur *BriefCam* : *"BriefCam extrait (…) les caractéristiques uniques du visage, telles que la distance entre les yeux, la largeur du nez et la forme des pommettes, qui sont les identifiants uniques de ce visage, et les code dans un vecteur de caractéristiques qui représente ce visage. Ce vecteur de caractéristiques est extrait à la fois pour les visages figurant sur une liste de surveillance et pour les visages que BriefCam détecte dans les séquences ».* Ce livre blanc figure en *annexe 8.*

- comme on va le voir, la reconnaissance faciale n'a jamais été la raison de l'acquisition du logiciel et les services ne l'avaient jamais appelée de leurs vœux ;

- la sous-utilisation du logiciel évoquée précédemment a mécaniquement réduit les risques d'utilisation irrégulière ;

- les images extraites des flux vidéo, qu'ils relèvent de la vidéo-protection (publique) ou de la vidéo-surveillance (privée) ne permettent que très rarement d'identifier directement un suspect. La qualité souvent médiocre des vidéos réquisitionnées (faits commis en soirée ou de nuit), et les *modus operandi* (visages masqués lors de vols à main armée) privent donc le plus souvent cette fonctionnalité d'utilité objective pour les officiers de police judiciaire, laquelle tient beaucoup plus, pour ceux-ci, à d'autres fonctionnalités fréquemment mises en œuvre, comme la recherche par similarités (couleur de véhicule, type de vêtements…). C'est ce qu'illustre l'exemple ci-dessous.

Encadré n°3 : utilité des logiciels d'analyse vidéo indépendamment de toute fonctionnalité de reconnaissance faciale

Dans le cadre d'une enquête visant à identifier et rechercher l'auteur d'une agression violente en scooter, les images de vidéoprotection de l'agression, trop éloignées de la scène et de qualité insuffisante ne permettent pas d'identifier visuellement l'auteur. Les enquêteurs observent toutefois qu'il est porteur d'un T-shirt bicolore, d'un graphisme particulier. C'est la fonctionnalité « similitude d'apparence » qui a donc été activée, avec la saisie judiciaire récurrente, dans les jours qui ont suivi l'agression, des vidéos de la ville, ensuite injectées dans *BriefCam*. Une séquence vidéo horodatée sur laquelle, près de dix jours après l'agression, apparaissait un individu portant un T-shirt identique à celui de l'auteur a, grâce à l'activation de cette fonctionnalité, été sélectionnée par *BriefCam*. Les investigations alors menées dans le secteur considéré permettront d'identifier et d'arrêter, sur le fondement de la similitude d'apparence, l'auteur de l'agression. L'emploi du logiciel et, en l'occurrence, de cette fonctionnalité, a été ici la condition *sine qua non* de l'interpellation de l'individu, à partir de l'injection systématique, sur réquisition judiciaire, pendant les jours ayant suivi l'agression, de centaines d'heures de vidéos saisies.

On notera pour achever sur les évolutions techniques du logiciel, qu'en raison de la polémique soulevée fin 2023 par cette problématique de la reconnaissance faciale, la société Canon, propriétaire de *BriefCam* a décidé, depuis le 1er janvier 2024, de retirer cette fonctionnalité des logiciels vendus sur le marché français.

2.2.2 Réalités de l'utilisation de la reconnaissance faciale du logiciel *BriefCam* par les forces de sécurité

2.2.2.1 La reconnaissance faciale n'est pas à l'origine de la demande d'achat du logiciel *BriefCam*

Il ne fait aucun doute que la fonctionnalité de reconnaissance faciale que comportent certaines versions de *BriefCam* n'est pas à l'origine de la demande d'acquisition de ce logiciel par les services d'enquête. Le besoin qu'ils exprimaient était de disposer d'un outil offrant un gain de temps dans l'exploitation des flux d'images vidéo. C'est l'existence, dans le logiciel *BriefCam*, d'une capacité de « dérushage », c'est-à-dire, comme on l'a vu, d'épuration des vidéos des séquences inutiles pour ne retenir que celles pouvant apporter des éléments utiles à l'enquête, qui a suscité l'intérêt des services et créé leur demande. C'est plus précisément le dispositif technique de *BriefCam* « SYNOPSIS » (cf. 1.1.2.2) et ses fonctionnalités de recherche multicritères qui a ont été considérés comme apportant une réelle valeur ajoutée à la conduite de l'enquête.

La problématique de la reconnaissance faciale ne s'est d'ailleurs posée que « passivement » comme on l'a expliqué précédemment et sa neutralisation n'est pas perçue comme un amoindrissement de son utilité pour les enquêteurs. Mais il est vrai aussi que les potentialités qu'offrirait dans l'enquête une fonctionnalité de reconnaissance faciale, si elle était légalement autorisée, susciterait évidemment l'intérêt des enquêteurs (cf. 3.2.2), dès lors que la qualité des images brutes en permettrait l'exploitation (par exemple pour la délinquance dans les transports en commun).

2.2.2.2 L'activation de la reconnaissance faciale : un cas unique dans une enquête judiciaire s'inscrivant dans un contexte exceptionnel

La mission n'a pas été matériellement en mesure de procéder à un contrôle informatique d'une éventuelle activation par les services utilisateurs de la fonctionnalité de reconnaissance faciale du logiciel *BriefCam*, contrôle qui n'aurait été possible qu'en cas de traçabilité exhaustive de l'exploitation du logiciel. En effet, selon l'éditeur du logiciel, la durée de conservation des données de connexion, inscrites dans le « journal d'audit », est limitée, par défaut, à 365 jours et ce « journal d'audit » ne trace pas l'activation par l'utilisateur des différentes fonctionnalités du logiciel[67].

La mission ne peut donc que s'en tenir aux déclarations des services lors des entretiens et aux documents reçus par la mission. Il en ressort, depuis 2015, un cas unique d'activation de la reconnaissance faciale (*annexe 9*), sur les 563 utilisations du logiciel dénombrées par la mission, qui sont un minimum.

En l'occurrence, dans le contexte exceptionnel des violences urbaines de l'été 2023, dans le cadre d'une enquête préliminaire, des photos (certaines étant issues du TAJ) d'individus susceptibles d'avoir participé aux violences ont été intégrées par les enquêteurs dans le logiciel. Des personnes ainsi soupçonnées sont alors apparues dans l'espace public, dans certaines séquences vidéo exploitées par le logiciel *BriefCam*. Mais les investigations complémentaires ont ensuite exclu leur implication. Ces personnes, dont le visage avait été « reconnu » par le logiciel et dont les enquêteurs connaissaient l'identité par le TAJ, n'ont donc pas été interpelées.

L'emploi de cette fonctionnalité de reconnaissance faciale n'a ainsi conduit à aucune mise en cause d'individus initialement soupçonnés, inscrite en procédure. Il s'est cependant fait hors cadre légal.

Sans préjudice de ce constat, ce cas unique d'activation de la reconnaissance faciale du logiciel *BriefCam* appelle trois observations :

- c'est l'activation irrégulière de la fonctionnalité de reconnaissance faciale qui a permis de confirmer, à partir des images vidéo saisies, la présence sur la voie publique et au moment des faits de personnes qui étaient soupçonnées. Mais c'est l'analyse humaine qui a conduit à ne pas les poursuivre, dès lors que les images n'attestaient pas de leur participation aux dégradations. Ce cas particulier apporte ainsi la démonstration que l'intervention humaine pour interpréter les images vidéo reste, *de facto*, incontournable, le logiciel se limitant, au mieux, à « reconnaître » mais étant incapable à ce jour d'une analyse du comportement pour lui attribuer, le cas échéant, une qualification pénale. Cette intervention humaine est *de jure* obligatoire, conformément au deuxième alinéa de l'article 47 de la loi n° 78-17 du 6 janvier 1978[68] ;

- le contexte de forte pression à l'élucidation de faits très graves (incendies de bâtiments publics, agressions de personnes dépositaires de l'autorité publique, pillages…) et à l'identification et la poursuite de leurs auteurs en vue d'une réponse pénale rapide peut sans doute expliquer sinon valider cet unique recours irrégulier à la reconnaissance faciale ;

- le cas d'espèce illustre enfin le paradoxe dans lequel se trouvent les services répressifs de ne pouvoir juridiquement utiliser des outils numériques pouvant pourtant contribuer efficacement, à charge comme à décharge, au recueil d'éléments de preuve objectifs d'infractions et à l'identification de leurs auteurs. On y reviendra en partie 3.

[67] Similitude d'apparence, reconnaissance de plaques, reconnaissance faciale, direction etc.

[68] *« Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel… »* Ce principe est au demeurant rappelé en police administrative, la loi « jeux olympiques et paralympiques » du 19 mai 2023, précisant explicitement que les traitements informatiques entrant dans son champ d'application *« ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite ».*

3 LA NECESSAIRE SECURISATION DE L'UTILISATION ET DE L'EXPERIMENTATION DE NOUVELLES TECHNOLOGIES NUMERIQUES PAR LES FORCES DE SECURITE

3.1 Organiser un contrôle interne et assurer une cohérence de doctrine pour la mise en oeuvre de nouvelles technologies numériques

3.1.1 Mettre en place un contrôle interne à triple finalité

3.1.1.1 Garantir l'expertise juridique

Comme on l'a vu en section 2.1.2.1, 8 années ont été nécessaires pour déterminer le régime juridique du logiciel *BriefCam* et les conséquences à en tirer en procédure. Personne ne peut s'en satisfaire. La multiplication prévisible des outils fondés sur l'IA et les risques induits pour les libertés individuelles obligent donc à accompagner toute acquisition sur le marché par les services de police et de gendarmerie de tels outils, d'une réflexion sur leur régime juridique, sans exclure pour autant d'opportunes initiatives de terrain. A ce propos, la doctrine de la DNPJ indique, sous la rubrique *« les achats de la filière »* : *« Les catalogues achats de la police nationale, élaborés par la direction des ressources humaines, des finances et des soutiens (DRHFS) en lien avec le service de l'achat, de l'innovation et de la logistique du MI (SAILMI), tiennent compte des besoins spécifiques exprimés par la filière police judiciaire. Dans les limites de sa dotation budgétaire, la filière peut se livrer à de la prospective technique ou technologique en sollicitant les acteurs du marché privé pour répondre à ses nouveaux besoins et tester des solutions innovantes dans le respect des règles de la commande publique »* [69]. A l'expérience des modalités d'acquisition, décrites en section 1.2.1.1, du logiciel *BriefCam* et du temps nécessaire à sa qualification de LRJ, on peut regretter que cette doctrine d'emploi limite la vigilance juridique aux seules règles de la commande publique, comme si « les solutions innovantes », c'est-à-dire numériques et de plus en plus fondées sur l'IA, ne nécessitaient pas aussi, et peut-être même surtout, une veille en matière de droit des données personnelles.

Cette expertise juridique, pour être assurée, doit d'abord être organisée et la réforme de la police nationale consécutive aux conclusions du Livre blanc de la sécurité intérieure devrait y contribuer.

Les nouvelles directions nationales, sous l'autorité du DGPN, qui *« exercent un contrôle permanent sur les conditions d'emploi des agents de leur filière conformément au cadre défini par la doctrine »*[70], et la désignation de directeurs zonaux, chacun étant notamment chargé du *« contrôle* [de] *l'activité de l'ensemble des directions et services de la police nationale sur son ressort de compétence »*[71] traduisent l'architecture du nouveau contrôle interne qui se met en place, dont la coordination et l'évaluation ont été confiés à l'IGPN, qui en élabore elle-même une doctrine d'emploi. Un service juridique a par ailleurs été créé au sein de la direction des ressources humaines, des finances et des soutiens (DRHFS), *« en complément du maintien et du renforcement des structures d'appui juridique dans chacun des services et directions nationales »*[72].

Bien entendu, le contrôle interne portera principalement sur le respect des règles de doctrine d'emploi. Mais le risque juridique, y compris lors de l'achat ou de la mise à disposition de nouveaux outils numériques, doit être pris en compte, notamment en s'appuyant sur ces nouvelles structures juridiques.

[69] Projet de « Doctrine de la direction nationale de la police judiciaire » (27 avril 2023).
[70] Selon le projet de « Doctrine applicable à la réforme de l'organisation et du fonctionnement des services centraux et territoriaux de la direction générale de la police nationale » (19 avril 2023).
[71] Même document.
[72] Certaines directions nationales se sont également dotées de départements numériques en charge de l'évaluation technique et juridique. Ces structures devront donc être systématiquement saisies avant toute nouvelle acquisition, en particulier de « solutions innovantes », à charge pour elles d'assurer le lien avec d'autres acteurs ministériels (conseillers juridiques et numériques du DGPN, de l'ANFSI, de la DLPAJ notamment), avec une attention particulière, aux fins de coordination, sur l'emploi de ces mêmes technologiques au sein de la gendarmerie nationale.

Concernant la gendarmerie nationale, les directions de la direction générale ainsi que le service de la transformation (ST)[73] disposent de leur propre service d'expertise juridique, compétent en matière de respect de la norme, notamment concernant les aspects numériques. La direction des opérations et de l'emploi (DOE) a récemment renforcé sa capacité d'expertise, avec la création de la mission juridique opérationnelle. Un travail d'identification des risques est par ailleurs régulièrement mis à jour, une cartographie de maîtrise des risques élaborée et une priorisation des actions à mener définie. C'est dans ce cadre qu'une veille des nouvelles technologies est mise en place pour anticiper les difficultés juridiques potentielles.

Le cadre institutionnel semble donc répondre à l'exigence de veille juridique qui s'impose aux directions métier. Mais au-delà de la structure, c'est surtout une culture portant essentiellement sur le droit des données personnelles qui doit être acquise et diffusée, notamment auprès des services de terrain, et devenir un réflexe à l'heure du développement de l'IA.

La mission appelle l'attention sur la nécessité, pour le ministère, de s'assurer que la multiplication des services juridiques ne se fasse pas au détriment de la cohérence de l'expertise[74].

Recommandation n°1 : Assurer une expertise juridique systématique et cohérente avant toute acquisition de nouvelles solutions numériques par les forces de sécurité (DGPN ; DGGN).

3.1.1.2 Assurer l'expertise technologique des produits achetés sur le marché

Acquérir des solutions numériques « sur étagère » est naturellement possible et dans certains cas souhaitable, voire indispensable[75]. Des précautions sont néanmoins à prendre.

Tout d'abord, si des initiatives de terrain sont à l'origine de projets d'acquisition de nouvelles solutions numériques, une validation hiérarchique doit être systématisée, précisément pour éviter des démarches insuffisamment sécurisées au plan juridique ou au plan de la stratégie d'équipement des services[76]. Dans un souci de cohérence dans les acquisitions de nouveaux équipements numériques des forces de sécurité et de respect de la politique de sécurité numérique du ministère de l'intérieur, les services territoriaux doivent ainsi rechercher systématiquement une validation technique au niveau central.

La présence auprès du DGPN d'un conseiller technologies et numérique et d'un service de la transformation numérique (STN) traduit d'ailleurs la volonté de cette institution d'améliorer le recensement des expressions de besoins, le pilotage des achats et globalement, de favoriser une plus grande intégration des solutions numériques du marché au « panier » technologique des directions-métier. De la même façon, outre le ST déjà mentionné, le DGGN dispose auprès de lui d'un officier général, conseiller à la stratégie digitale et technologique, qui pilote une commission chargée d'évaluer et hiérarchiser la totalité des projets numériques de la gendarmerie nationale.

Mais au-delà de ces architectures institutionnelles, c'est bien une culture de remontée systématique au niveau central des souhaits des services territoriaux d'acquisition de nouvelles solutions numériques qui doit être acquise.

[73] Placé sous l'autorité directe du DGGN, le ST dispose de juristes spécialisés, notamment du référent informatique et liberté et du responsable de l'administration des données.
[74] Comme le relève le Document d'orientation stratégique de la DRHFS de la DGPN, *« la fonction juridique centrale de la police nationale apparaît dispersée (…) pourtant, l'activité de police est de plus en plus organisée, normée et déterminée, par les règles de droit, qu'elle doit maîtriser et ajuster à ses besoins opérationnels »* (19 avril 2023, partie 5).
[75] Outre *BriefCam*, le SNPS, par exemple, dispose d'autres solutions numériques commerciales pour conduire son action. Ainsi la solution d'analyse vidéo *Augmented Vision*, développée par le groupe IDEMIA, dont les performances pourraient être supérieures à celles de *BriefCam*. Une licence de ce logiciel est en cours d'acquisition au SNPS, où son installation est prévue en avril 2024 - hors reconnaissance faciale -, sous couvert d'une AIPD en cours de réalisation.
[76] Compte tenu des questions de transparence qu'elle peut poser, toute mise à disposition, surtout gratuite, de produits par des entreprises privées à des fins de test ou d'essais doit être explicitement autorisée par la hiérarchie, avec une information systématique de l'administration centrale.

Recommandation n°2 : Organiser au niveau central l'évaluation technique des solutions numériques dont l'acquisition est envisagée par les directions et services (DGPN ; DGGN).

Ensuite, toujours au niveau territorial, une double démarche de renforcement de la connaissance technologique devrait être assurée : au sein des forces d'abord, une prise en compte bien documentée des besoins techniques des enquêteurs par les référents-sûreté des services pourrait permettre à ces derniers d'améliorer le dialogue technique qualitatif avec les maîtres d'ouvrage, pour le choix des équipements d'intérêt partagé ; ensuite, la vision des référents-sûreté des préfectures sur les équipements numériques de sécurité des collectivités locales pourrait être améliorée et complétée, en lien avec les forces de police et de gendarmerie, pour assurer la mise à jour de la cartographie de la vidéoprotection et la bonne connaissance par les forces de sécurité de l'Etat des moyens numériques des collectivités locales liés à la surveillance vidéo.

3.1.1.3 Rationaliser et sécuriser les acquisitions de nouveaux outils numériques par les forces de sécurité

La mission n'a pas pu consolider les montants consacrés par la police et la gendarmerie nationales à l'acquisition du logiciel Briefcam entre 2015 et 2023, les achats ayant été faits selon des modalités diverses, parfois concomitamment : dans certains cas, sur une base annuelle mais reconduite, centralisés ou non, dans d'autres cas, sur bons de commandes parallèles avec des fournisseurs différents (UGAP et *M2M Factory*), parfois encore (au seul bénéfice d'une partie des services de la gendarmerie), dans le cadre d'un marché de sécurité.

Il apparaît donc nécessaire d'organiser pour les acquisitions d'outils numériques nouveaux, un processus d'achats formalisé, permettant leur sécurisation et leur rationalisation et identifiant les rôles des différents acteurs, à l'instar des achats plus traditionnels ou récurrents. L'évaluation du besoin et de la dépense conditionne en effet « le bon achat ».

Lorsqu'il s'agit d'expérimenter un nouveau produit, la désignation coordonnée d'un service testeur devrait être privilégiée, notamment pour arrêter le calendrier de la décision d'achat. De même, le dénombrement des licences à acquérir doit résulter d'une centralisation des expressions de besoin des services. Ces exigences imposent non seulement une action centralisée de recensement du nombre des acquisitions à réaliser, mais également une prise en compte *ab initio* des modalités précises du maintien en conditions opérationnelles des produits achetés (coût de leur maintenance, calendrier de leur mise à jour etc.). Le cas particulier du logiciel *BriefCam* montre qu'il n'y a eu aucune anticipation pluriannuelle des besoins de mise à jour et de maintenance, conduisant à une très forte hétérogénéité des équipements des services et à des décisions de cessation d'utilisation commandées par des raisons budgétaires plus qu'opérationnelles. Une exacte appréciation des coûts, enfin, doit sécuriser la procédure d'acquisition à choisir et le respect des seuils de la commande publique (marché ouvert avec mise en concurrence, procédure de gré à gré, achats sur bons de commande auprès de l'UGAP…).

Le choix des ressources budgétaires à mobiliser doit, quant à lui, être prioritairement fondé sur la nature des produits et sur leur cycle de vie. Ainsi, les fonds de concours de l'AGRASC et de la MILDECA - fortement mobilisés dans le cas du logiciel *BriefCam* -, qui sont, par construction, annuels et non pérennes, doivent être privilégiés pour des dépenses *« one shot »* et de court terme ou à des fins de test. Les dépenses correspondant à des produits relevant d'une logique de récurrence ou de marchés pluriannuels doivent quant à elles être engagées sur les programmes budgétaires (176 et 152 au cas d'espèce), afin de garantir une présentation sincère et exhaustive ainsi que la disponibilité et l'homogénéité des moyens mis à disposition.

Le contrôle interne doit donc intégrer également la dimension achat.

Recommandation n°3 : Organiser un processus d'achat formalisé et sécurisé pour l'acquisition de nouvelles solutions numériques (DGPN ; DGGN avec la DEPAFI – SAILMI).

La mission a par ailleurs constaté un décalage important, bien sûr explicable, entre la connaissance et le suivi des outils numériques souverains pouvant intéresser les forces de sécurité, notamment pour les missions de police judiciaire, et celle des produits du marché. Par construction, les produits souverains sont maîtrisés, puisqu'ils correspondent en principe à des expressions de besoin des utilisateurs de l'Etat. En revanche, les produits du marché ne semblent pas faire l'objet d'un recensement, ni d'un suivi, ni d'une veille organisée, *a fortiori* si leur utilisation se fait hors réseau informatique ministériel.

L'organisation de ce suivi et de cette veille paraît souhaitable, pour éviter les initiatives ponctuelles sinon personnelles, comme cela a pu se produire dans le cas du logiciel *BriefCam*. L'agence du numérique des forces de sécurité intérieure (ANFSI) paraît légitime pour remplir ce rôle. L'intranet du ministère pourrait donner des informations régulières sur cette veille technologique, pour la bonne information des services territoriaux.

Par ailleurs, les principaux éditeurs ou opérateurs, connus de l'Etat, devraient se voir désigner des interlocuteurs au niveau central. A la DGPN, les nouveaux services numériques créés au sein des directions métier pourraient ainsi être désignés.

Recommandation n°4 : Organiser au niveau central un suivi et une veille technologiques sur les produits du marché pouvant intéresser les forces de sécurité (DGPN ; DGGN ; ANFSI).

3.1.2 Assurer l'indispensable cohérence de doctrine sur la mise en oeuvre des technologies numériques d'aide à l'enquête par la police et la gendarmerie nationales

Comme on l'a vu, le très faible nombre de licences du logiciel *BriefCam* acquises par les forces de sécurité, doublé de la très faible utilisation de ce logiciel (toujours *a posteriori* et dans un cadre judiciaire) et le cas unique, en huit années, d'activation irrégulière par un service de la fonctionnalité de reconnaissance faciale sont très éloignés de la dramatisation sous-tendant l'article de Disclose.

Très vigilantes, par expérience, sur les polémiques accompagnant régulièrement la mise en œuvre de fichiers, traitements et produits ou systèmes d'information numériques en matière de sécurité, les deux directions générales[77] ont adopté des stratégies différentes en matière d'officialisation juridique de ce logiciel et délivré à leurs services, en ordre dispersé, des instructions pouvant certes s'expliquer par le recours au principe de précaution, mais dont la logique interroge.

Ce constat traduit un manque de cohérence de doctrine d'autant plus contre-productif qu'on est, précisément, dans un contexte de polémique.

3.1.2.1 Des choix différents d'officialisation du logiciel *BriefCam*

Si la reconnaissance comme logiciels de rapprochement judiciaire relevant du décret n° 2012-687 du 7 mai 2012, des logiciels d'analyse vidéo en usage ou en gestation au sein de la police et de la gendarmerie nationales a été longue (cf. 2.1.2), les deux directions générales n'ont adopté une démarche convergente d'officialisation que pour le seul logiciel souverain *Système V*, avant son déploiement dans 7 services pour expérimentation. Déclaré le 25 juillet 2023 par la DGPN[78], *Système V* l'a été le 20 novembre de la même année par la DGGN.

Pour le logiciel *BriefCam*, elles ont en revanche fait des choix différents. La DGPN, après la publication de l'article de Disclose, l'a déclaré comme LRJ le 14 décembre 2023[79]. La DGGN, quant à elle, selon laquelle, pourtant, *« le déploiement* [de *BriefCam*] *s'est effectué dans le cadre des*

[77] Pour lesquelles *BriefCam* était au demeurant un objet marginal et mal identifié.
[78] En application du IV de l'article 31 de la loi « informatique et libertés », accompagné d'une analyse d'impact relative à la protection des données (AIPD).
[79] L'AIPD qui l'accompagne fait d'ailleurs explicitement allusion cet article.

articles 230-20 et suivants du code de procédure pénale [réglementant les LRJ] »[80] n'a pas procédé à cette régularisation juridique. Cette abstention[81] peut s'expliquer par une décision formalisée le 17 novembre 2023 – après publication de l'article de Disclose – par le DOE de cette direction générale, de *« suspendre »* immédiatement toute utilisation du logiciel pour *« des raisons d'insécurité juridique »*. Mais cette insécurité juridique, incontestable à défaut d'engagement de conformité auprès de la CNIL, aurait pu être rapidement levée, comme l'a fait la DGPN, par la production de cet engagement de conformité, assorti d'une AIPD d'autant plus aisée à réaliser que son « modèle » était celui de l'AIPD de *Système V*, formalisé le 20 novembre.

On en déduit donc que ce choix de non régularisation par la DGGN du logiciel *BriefCam* (à la différence de *Système V*), se traduisant par l'arrêt total de son emploi par les services enquêteurs de la gendarmerie nationale, est totalement assumé à la lumière des explications ci-dessus rappelées.

3.1.2.2 Une communication interne différenciée concernant la reconnaissance faciale

Avant même la régularisation, partielle comme on vient de le dire, du logiciel *BriefCam* comme LRJ, les deux directions générales avaient choisi des démarches différentes de communication et d'instructions internes concernant la fonctionnalité de reconnaissance faciale.

Dans un courriel du 6 février 2023 aux directions et services affectataires de BriefCam, très antérieur à la publication de l'article de Disclose, la DGPN rappelait formellement, par précaution, la prohibition d'utilisation de la fonctionnalité de reconnaissance faciale, sous quelque dénomination que ce soit : *« quel que soit le logiciel* [de rapprochement judiciaire]*, il est interdit de recourir à un quelconque dispositif de rapprochement de visages ou de reconnaissance faciale »*.

La DGGN n'a pas procédé à ce rappel juridique, certes de précaution. Cette abstention n'est évidemment en aucun cas l'expression d'une quelconque tolérance de cette direction générale par rapport à un éventuel recours, hors cadre légal, à la reconnaissance faciale. On ne peut exclure cependant que la formalisation de ce rappel, à l'identique de la DGPN, aurait pu au moins avoir une vertu pédagogique.

Sur des problématiques juridiques identiques concernant le même logiciel utilisé en police comme en gendarmerie, *a fortiori* sur une thématique aussi politiquement sensible que la reconnaissance faciale, on peut s'étonner de ces différences de méthodes entre les deux forces. Elles font apparaître un défaut de coordination et peut-être, d'abord, de dialogue, qui peut *a minima* brouiller, ne serait-ce qu'au plan institutionnel, la lisibilité de l'emploi par les FSI d'outils numériques identiques mis à leur disposition. Assurer une unité de doctrine des deux forces sur la gestion de solutions numériques d'une particulière sensibilité en matière de libertés individuelles est donc un impératif pour le ministère.

Recommandation n°5 :	**Assurer une unité de doctrine de la police et de la gendarmerie nationales sur la définition du cadre juridique des nouvelles technologies numériques et sur leur doctrine d'emploi (DGPN et DGGN).**

3.1.2.3 Un choix identique, mais difficilement compréhensible, de suspendre toute utilisation du logiciel *BriefCam*

Comme on vient de le voir, la DGGN a, depuis le 17 novembre 2023, suspendu toute utilisation du logiciel *BriefCam* par les unités de la gendarmerie, dans l'insécurité juridique qu'elle ne prend pas l'initiative de lever sur le statut du logiciel.

[80] Note communiquée à la mission.
[81] Peut-être motivée par les perspectives de déploiement de Système V dans une trentaine d'unités en 2024.

La DGPN reste, quant à elle, sur un choix plus surprenant, puisque, après avoir procédé à la régularisation juridique du logiciel auprès de la CNIL, elle a néanmoins donné instruction d'en suspendre toute utilisation dans l'attente des conclusions du présent rapport.

La mission prend acte de cette régularisation, opportune, qui autorise légalement les services de police judiciaire à mettre en œuvre ce nouveau LRJ, sur l'autorisation, comme le prévoit le code de procédure pénale, et sous le contrôle de l'autorité judiciaire. La logique du maintien de cette suspension d'emploi est en revanche difficilement perceptible. Elle prive surtout les enquêteurs, sur le terrain, d'un potentiel important d'élucidation d'affaires. Pour la gendarmerie, le SCRC a ainsi indiqué à la mission que la suspension d'utilisation avait conduit ce service à refuser la sollicitation de trois ou quatre SR, pour une aide à l'exploitation de flux vidéo. Des services seront ainsi conduits à renoncer à toute exploitation d'images de surveillance vidéo, dès lors qu'elles représentent un nombre d'heures de visionnage « manuel » trop important.

La mission estime donc que, s'agissant de la police nationale, et dès lors que toutes les démarches de régularisation juridique du logiciel *BriefCam* ont été assurées par cette direction générale, rien ne s'oppose à son utilisation par les services enquêteurs de cette force, bien entendu en dehors de toute activation de la fonctionnalité de reconnaissance faciale - jusqu'à ce qu'un cadre légal d'utilisation de cette fonctionnalité dans les logiciels de rapprochement judiciaire soit défini -.

La levée de cette interdiction d'utilisation paraît d'autant plus nécessaire que, comme on l'a dit, le logiciel *Système V*, qui doit remplacer *BriefCam*, ne sera déployé, selon un schéma pluriannuel, qu'à compter de l'été 2024 au plus tôt.

Recommandation n°6 : Lever sans délai la suspension d'utilisation du logiciel *BriefCam* par les services enquêteurs de la police nationale (DGPN).

D'une manière plus générale, la mission considère que, pour conforter la capacité opérationnelle des services enquêteurs, à laquelle contribuent les logiciels d'analyse vidéo, le logiciel *BriefCam* devrait, au prix de sa régularisation juridique par la DGGN, être maintenu dans tous les services d'enquête, en police comme en gendarmerie, jusqu'à son remplacement par *Système V*, pour éviter toute solution de continuité entre ces deux outils d'aide à l'enquête.

Recommandation n°7 : Poursuivre l'utilisation du logiciel *BriefCam* dans les services d'enquête, jusqu'à son remplacement par le logiciel *Système V* (DGPN ; DGGN).

3.2 Imaginer un cadre légal d'expérimentation de nouvelles technologies numériques par les forces de sécurité intérieure

L'acquisition du logiciel *BriefCam* par les forces de sécurité, poussées par des évènements dramatiques et imprévisibles, alors qu'aucun produit souverain ne permettait encore l'analyse rapide mais indispensable de milliers d'heures d'images vidéo, illustre de façon très concrète le besoin dans lequel peuvent se trouver les forces de sécurité de recourir à des produits numériques, disponibles sur le marché, susceptibles de leur permettre d'exercer avec le maximum d'efficience les missions qui leur sont confiées.

Même si *BriefCam* n'a pas été acheté par le ministère de l'intérieur dans une démarche d'expérimentation au sens de l'article 37-1 de la Constitution, d'autres outils informatiques, notamment mettant en œuvre l'IA (cf. 3.2.2), sont susceptibles d'apparaître rapidement dans le paysage numérique, dont certains présenteront certainement des fonctionnalités pouvant être exploitées pour l'exercice des missions de sécurité[82].

[82] Le Livre blanc de la sécurité intérieure de 2020 indique à cet égard que *« dans le domaine clef des biométries, plusieurs chantiers sont à engager ou intensifier (rénovation des formes traditionnelles et intégration de nouvelles capacités liées à l'IA) par l'adoption d'une approche multibiométrique »*. Il consacre par exemple d'importants développements à la biométrie du visage, mais également à la biométrie vocale et à l'odorologie (points 4.5 et 4.6, p. 260 et suiv.).

Dans le champ de ces dernières, les outils numériques sont, par construction, susceptibles de porter atteinte aux libertés publiques et individuelles. Leur usage est donc réglementé par la loi « informatique et libertés ». Mais cette loi, conçue à une époque où l'informatique se réduisait aux fichiers, offre un cadre rigide, très fortement normé, obéissant à une logique binaire (interdit/autorisé) avec, pour les traitements de souveraineté, qui recueillent et exploitent souvent des données sensibles au sens de cette loi, un recours presque systématique au décret en Conseil d'Etat après avis de la CNIL, désormais accompagné d'une AIPD. Ce cadre rigide n'est pas adapté à la mise en œuvre de procédures d'expérimentation de nouveaux outils numériques, appréhendés *in abstracto* par les services possiblement intéressés, puisque non encore mis en œuvre, incomplètement mesurés dans leurs potentialités et dans les risques qu'ils peuvent donc présenter pour les libertés. L'expérimentation, au sens de l'article 37-1 de la Constitution, nécessite au contraire réactivité, souplesse et agilité.

Le développement de l'IA, dont l'usage par les forces de sécurité ne peut que se développer et dont les risques sont encore mal évalués, offre l'opportunité, comme on le verra en section 3.2.2, de construire un cadre légal d'expérimentation pouvant avoir des applications très concrètes pour la mise en œuvre par les forces de sécurité, dans un environnement juridique clair, de nouveaux outils informatiques n'entrant dans aucun cadre normatif.

3.2.1 Esquisse de définition d'un cadre légal d'expérimentation pouvant bénéficier aux forces de sécurité

Les besoins d'expérimentations, fortement accélérés par les transformations numériques, se sont multipliés depuis une vingtaine d'années dans tous les champs de l'action publique.

Dans son étude de 2019[83], le Conseil d'Etat relevait que, depuis la réforme constitutionnelle de 2003[84], l'action régalienne de l'Etat était, avec l'action sociale et l'éducation nationale, l'un des trois domaines d'élection de ces expérimentations, et notamment *« l'exercice de nouveaux modes d'action opérationnels des forces de l'ordre »*[85], comme l'analyse vidéo étudiée dans ce rapport.

Les cas d'expérimentations, nombreux en effet, concernant presque tous la mise en œuvre des « caméras-piéton », ressemblent à un catalogue « à la Prévert ». En deux ans et demi, 5 dispositions législatives ont été adoptées[86], dans des termes analogues ou comparables, pour une finalité unique : permettre aux agents des forces en charge d'une mission de secours ou de sécurité d'enregistrer les images de leurs interventions au moyen de caméras individuelles.

Ce bilan n'est pas satisfaisant : une disposition législative-cadre, posant en facteurs communs le principe, les règles et les garanties d'emploi des caméras-piéton, sur la base de laquelle des textes réglementaires auraient précisé les services concernés et leurs éventuelles spécificités d'emploi de ces matériels aurait fait l'économie de 5 débats parlementaires, au contenu récurrent.

Dans cette logique, il paraît souhaitable d'introduire dans la loi « informatique et libertés » un dispositif cadre permettant les expérimentations, dans l'esprit d'ailleurs du RGPD[87], dont le paradigme est différent de celui de la loi du 6 janvier 1978 en ce qu'il transfère largement la responsabilité de la mise en œuvre des traitements à leurs responsables, en préférant à un contrôle *a priori* systématique des Etats – qui caractérise encore la loi de 1978 - un régime de contrôle *a posteriori*, assorti de sanctions en cas de manquements.

---

[83] *« Les expérimentations : comment innover dans la conduite des politiques publiques ? ».*

[84] La loi constitutionnelle n° 2003-276 du 28 mars 2023, codifiant en quelque sorte les jurisprudences antérieures du Conseil d'Etat et du Conseil constitutionnel, a prévu dans le nouvel article 37-1 que *« la loi et le règlement peuvent comporter, pour un objet et une durée limités, des dispositions à caractère expérimental ».*

[85] P.24 et 25.

[86] Les agents et services concernés sont respectivement : les agents de services de sécurité de la SNCF et de la RATP (loi n°2016-339 du 22 mars 2016, art.2) ; les agents de police municipale (loi n°2016-731 du 3 juin 2016, art.114) ; les agents des forces de sécurité de l'Etat pour les contrôles d'identité auxquels ils procèdent (loi n°2017-86 du 27 janvier 2017, art.211) ; les sapeurs-pompiers professionnels et volontaires (loi n°2018-697 du 3 août 2018, art.1er) et, dans le champ du ministère de la justice, les agents de l'administration pénitentiaire (même loi, art.2).

[87] Et, comme on le verra en section 3.2.2, du projet de Règlement européen sur l'IA.

La mission ne peut, dans le cadre de ce rapport, qu'esquisser brièvement, en ayant particulièrement à l'esprit son application aux nouvelles solutions numériques d'action opérationnelle des forces de sécurité, notamment en police judiciaire[88] (cf. 3.2.2), quelques pistes de réflexion sur un tel régime-cadre d'expérimentation, qui nécessiteraient évidemment une analyse juridique approfondie.

En premier lieu, l'insertion dans la loi de 1978 d'un dispositif autorisant les expérimentations s'adosserait à l'article 37-1 de la Constitution. Il aurait essentiellement pour but d'alléger le cadre réglementaire strict, facteur de lenteur, s'imposant à tous les traitements de sécurité publique ou ayant pour objet la recherche et la poursuite des auteurs d'infractions.

Rappelons qu'en application de l'article 31 de la loi, *« les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et : 1° qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; 2° ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté »* nécessitent l'avis préalable, motivé et publié de la CNIL. Depuis l'entrée en vigueur de la directive « police-justice », les traitements concernés nécessitent également la réalisation d'une AIPD. En application du II de l'article 31, ceux traitant de données dites « sensibles », au nombre desquelles, notamment, les *« données génétiques,* [ou] *biométriques aux fins d'identifier une personne physique de manière unique »* exigent en outre un décret en Conseil d'Etat, les autres relevant d'un arrêté ministériel. A l'heure du développement de la biométrie dans de multiples solutions informatiques, par exemple pour certains traitements d'analyse vidéo comme *BriefCam* (cf. supra 2.2.1.1), l'exigence d'un décret en Conseil d'Etat est donc générale[89].

Dans la pratique, ce régime d'élaboration des actes réglementaires, notamment des décrets en Conseil d'Etat, suppose un temps long, encore allongé par l'exigence généralisée d'AIPD. Les délais, au minimum de plusieurs mois, sont même, pour de nombreux traitements de sécurité, de plusieurs années, avant que les forces de sécurité soient légalement autorisées à les utiliser[90].

Ce sont sans doute les produits numériques souverains, comme le TAJ, le FNAEG, le FNAED ou ACCRed, déjà cités, qu'avait en tête le législateur dans la définition de ce régime très normé d'autorisation, évidemment commandé par le souci de protection des libertés. Ces traitements souverains peuvent, dans une certaine mesure, faire l'objet d'anticipation et s'accommoder d'un dialogue de long terme avec la CNIL. Mais l'apparition sur un marché caractérisé par l'innovation permanente, de nombreux produits numériques reposant de plus en plus fréquemment sur l'IA, qui peuvent potentiellement répondre à des besoins urgents des forces de sécurité (comme ce fut le cas de *BriefCam*) pose en termes nouveaux la problématique de la procédure d'élaboration des textes d'autorisation des traitements de données personnelles, en particulier lorsqu'il s'agit de les expérimenter pour les évaluer techniquement avant de les généraliser.

[88] Selon le Conseil d'Etat dans son étude précitée de 2019, *« a priori aucun secteur n'est exclu du champ de l'expérimentation ». « Le Conseil d'Etat et le Conseil constitutionnel ont même confirmé l'éligibilité de la matière pénale* [à l'expérimentation], *à condition que la loi ou le décret en fixent l'objet et les conditions de manière suffisamment précise »* (p.16).

[89] A titre d'exemple, si en tant que simple LRJ relevant du décret du 7 mai 2012, *Système V* ne relève que d'un simple engagement de conformité auprès de la CNIL, sans acte réglementaire préalable d'autorisation, il en va autrement s'il doit comporter dans l'avenir la mise en œuvre d'une fonctionnalité de reconnaissance faciale reposant sur la biométrie, comme l'envisage le ministère de l'intérieur. Dans cas, c'est donc un décret en Conseil d'Etat qui devra être pris, après avis de la CNIL.

[90] D'un point de vue strictement juridique, la CNIL dispose d'un délai de 2 mois pour se prononcer sur les projets de traitements qui doivent lui être soumis. Ce délai est prorogeable une fois, portant le temps potentiellement incompressible à 4 mois. Mais dans les faits, surtout pour les traitements les plus sensibles, ou les plus sujets à polémique, le Gouvernement ne prend pas le risque de considérer que le silence éventuel de la CNIL au bout de 4 mois vaut avis. Pour tous ces traitements, et pour minimiser les risques juridiques, il prend le parti d'attendre un avis formel de l'autorité de contrôle.

S'il doit être procédé à des expérimentations, comme cela paraît souhaitable pour des raisons de sécurité technologique, juridique et de bonne gestion financière, le cadre légal rappelé ci-dessus constitue donc aujourd'hui un frein insurmontable. Au surplus, le traitement à expérimenter étant, par hypothèse, nouveau, la rédaction d'une AIPD rigoureusement documentée constitue une gageure, puisque les risques dudit traitement sur la protection de la vie privée et des libertés ne peuvent être exactement mesurés avant sa mise en œuvre.

Une disposition cadre autorisant la mise en œuvre expérimentale de nouvelles technologies numériques pourrait donc utilement trouver sa place dans la loi du 6 janvier 1978. Si, dans le respect de la hiérarchie des normes, aucune expérimentation qui mettrait en cause des règles et principes de niveau législatif ne pourrait être conduite sans modification expresse de la loi, une disposition sur l'expérimentation des traitements soumis à autorisation réglementaire pourrait en revanche alléger fortement leurs contraintes réglementaires, dès lors que la loi fixerait ou rappellerait les principes fondamentaux auxquels ne pourraient en aucun cas déroger les expérimentations.

Au lieu d'une autorisation formelle par arrêté ou décret en Conseil d'Etat, pris après avis de la CNIL, c'est à dire nécessitant un délai incompressible d'instruction par l'autorité de contrôle et la Haute Assemblée, un régime de déclaration à la CNIL de la mise en œuvre expérimentale d'un nouveau traitement de données personnelles pourrait être envisagé, assortie d'un descriptif complet, d'une présentation des finalités poursuivie et des entités expérimentatrices, ainsi que d'un nouveau type d'engagement de conformité : l'engagement de conformité aux principes fondamentaux évoqués ci-dessus[91] .

Cette déclaration transférerait, dans l'esprit de la réglementation européenne des données personnelles, la responsabilité de la mise en œuvre du traitement à son responsable juridique, qui en assumerait toutes les conséquences de droit. La déclaration et son engagement de conformité devraient être accompagnés d'une AIPD, mais qui pourrait être simplifiée compte tenu de la connaissance embryonnaire, par hypothèse de raisonnement, de ce nouveau produit, quitte à être enrichie en cours d'expérimentation. Les traitements de données relevant aujourd'hui du décret en Conseil d'Etat, c'est-à-dire ceux traitant de données « sensibles », pourraient être autorisés, aux fins et pour le temps de l'expérimentation, par arrêté ministériel, le cas échéant, pour des raisons de sécurité juridique, au bénéfice d'une demande d'avis du Gouvernement au Conseil d'Etat, avis qui serait publié par exigence de transparence.

S'agissant des conditions de leur mise en œuvre, ces nouveaux traitements expérimentaux devraient bien entendu respecter les règles de procédure qui pourraient leur être applicables. Ainsi, les outils numériques expérimentaux ayant un « statut » en procédure pénale, comme de nouveaux LRJ, devraient, conformément au régime de ces derniers, être autorisés par le magistrat, pendant le temps de l'expérimentation, et être contrôlés par lui. Il serait ainsi dérogé à titre expérimental aux règles d'autorisation desdits traitements de données personnelles, mais non aux règles procédurales d'usage de ces traitements, ce qui renforcerait d'ailleurs l'efficience de l'expérimentation.

L'acceptabilité d'une procédure ainsi simplifiée supposerait évidemment que les expérimentations soient sans *a priori*, plus précisément sans idée préconçue de la pertinence du dispositif expérimenté, ce qui n'a pas toujours été le cas, notamment dans le champ régalien. Comme l'indique le Conseil d'Etat dans son étude de 2019, *« l'expérimentation n'a de sens que parce que le décideur public fait face à une incertitude qui l'empêche de prendre, immédiatement* (…)*, une décision qu'il saurait être la meilleure »*[92].

Les expérimentations de ce nouveau cadre devraient aussi respecter les lignes directrices de la méthodologie de conduite et d'évaluation dégagée par le Conseil d'Etat dans la deuxième partie de cette même étude de 2019. La mission insiste sur le fait que les expérimentations doivent disposer

[91] Se distinguant donc de ceux prévus au IV de l'article 31 de la loi.
[92] P.12.

d'un temps suffisant de mise en œuvre pour que des conclusions puissent en être utilement tirées : rien ne devrait exclure, dans les cas complexes, des expérimentations sur plusieurs années, le cas échéant assorties de bilans d'étapes.

L'évaluation de l'expérimentation doit surtout être transparente, ce qui suppose qu'elle ne soit pas réalisée en vase clos[93]. Pour les traitements relevant de la police judiciaire, la présidence d'un comité d'évaluation par un haut magistrat, en activité ou honoraire, serait ainsi un gage de rigueur et d'indépendance. L'association étroite de la CNIL serait évidemment indispensable, sans préjudice bien sûr de ses pouvoirs permanents de contrôle et de sanction. On pourrait même envisager de solliciter des associations ou des organismes habituellement réservés sinon hostiles à la mise en œuvre de tout traitement de données personnelles, notamment, de « données sensibles » par les forces de sécurité. Il leur appartiendrait alors d'accepter ou non cette participation aux évaluation, dans le respect de leur liberté de pensée et d'expression, mais aussi de l'exigence de confidentialité de certaines informations et des cas d'usage des technologies ainsi expérimentées.

Au bénéfice de ces quelques lignes directrices, une démarche d'élaboration d'un dispositif cadre d'expérimentation de nouvelles technologies numériques par la police et la gendarmerie nationales semble désormais d'autant plus souhaitable que le projet de Règlement européen sur l'IA en offrira prochainement l'opportunité.

3.2.2 S'adosser au futur Règlement européen sur l'IA pour fixer un cadre d'expérimentation de nouvelles technologies numériques dans le champ de la sécurité

Le traitement des données dans le champ régalien de la sécurité est explicitement réglementé par les textes communautaires et nationaux. Si, au sein des activités de sécurité, les activités judiciaires échappent au RGPD[94], elles sont en revanche spécifiquement prises en compte dans la directive « police-justice » et, en droit national, dans la loi du 6 janvier 1978. Selon ces textes, la prévention, la recherche, la constatation et la poursuite des infractions pénales constituent un « intérêt public »[95], justifiant un régime d'autorisation de traitements de données personnelles mis en œuvre pour le compte de l'Etat[96].

Le Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union (dont le RGPD et la directive police-justice), dont le texte de compromis a été adopté le 9 décembre 2023 au terme de la phase de « trilogue », et qui devrait être définitivement adopté en avril prochain, constitue une opportunité d'évolution et d'assouplissement de notre droit interne, du fait du nouveau cadre de réflexion qu'il propose sur les traitements de données intégrant de l'IA dans un intérêt public, au sein duquel se trouve donc le champ judiciaire[97]. Il propose en effet un dispositif d'encadrement d'expérimentations, dont pourraient s'inspirer des évolutions normatives internes désormais souhaitables, comme on vient de le rappeler.

Ce projet de Règlement repose sur le constat que l'IA est porteuse d'opportunités dont on ne peut se priver et conclut à la nécessité de réglementations souples, pour tenir compte du rythme des innovations technologiques, sans préjudice d'un encadrement strict pour la protection des droits et libertés fondamentaux.

---

[93] *« Le choix d'un évaluateur qui présente des garanties d'impartialité pour assurer l'objectivité des analyses n'est que rarement effectué. La grande majorité des expérimentations sont encore évaluées par les administrations pilotes et les observations des publics destinataires de l'expérimentation (usagers du service public, citoyens) sont peu sollicitées. Par exemple, la direction générale de la police nationale (DGPN) évalue directement ses propres expérimentations, à l'image de celle conduite entre 2017 et 2018 sur le port de caméras mobiles par les policiers et gendarmes à l'occasion de contrôles d'identité* » (Etude du Conseil d'Etat déjà citée, p.38).

[94] Cf. d) du 2° de l'article 2.

[95] III de l'article 6 de la loi du 6 janvier 1978.

[96] 2° du I de l'article 31.

[97] 1a. de l'article 54, étant précisé qu'à la date de rédaction du présent rapport, la version de compromis du projet de Règlement n'existe qu'en langue anglaise.

Au plan juridique, les systèmes d'IA considérés « à haut risque » pour les droits fondamentaux, catégorie dans laquelle sont explicitement rangés les systèmes utilisés dans le cadre judiciaire[98] nécessitent, à la charge du « fournisseur », une appréciation et une évaluation strictes de l'objectif recherché, une documentation et une information exhaustives tout au long du cycle de vie du système, ainsi qu'une traçabilité totale des traitements. Les Etats membres pourront par ailleurs confier à une autorité de contrôle, comme, en France, la CNIL, un contrôle de ces processus.

Importante clarification, dans les systèmes d'IA relevant du judiciaire, le recours à la biométrie aux fins d'identification *a posteriori*, par comparaison des images avec des bases de données définies par les autorités répressives est explicitement autorisé, au bénéfice d'un encadrement strict, et notamment d'une autorisation judiciaire[99]. Cette clarification juridique devrait permettre, sous réserve de cet encadrement strict, une utilisation de la reconnaissance faciale dans la procédure judiciaire allant, en droit interne, au-delà de la seule exploitation du TAJ. Elle pourrait ainsi légitimer l'introduction contrôlée de la reconnaissance faciale dans des LRJ, voie dans laquelle s'est engagé le ministère de l'intérieur dans le cadre du droit national.

Ce règlement s'inscrit enfin dans une logique ouverte d'expérimentation de dispositifs d'IA, en autorisant des tests en conditions réelles[100].

Même si ce nouveau Règlement européen n'a pas été définitivement adopté à la date de ce rapport, il ouvre des perspectives d'évolutions du droit des données numériques interne au moins aussi importantes que celles qu'offrait, en 2016, le RGPD, parmi lesquelles l'expérimentation de nouvelles technologies numériques.

Ces opportunités d'évolution du droit interne, tout particulièrement sur l'IA, avaient d'ailleurs été soulignées par le Conseil d'État dès 2022, qui mettait l'accent sur *« l'opportunité d'anticiper l'entrée en vigueur du règlement IA »* afin de *« conduire une stratégie volontariste de déploiement de l'IA publique de confiance »*[101].

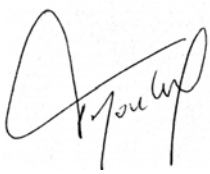
Un régime légal clair et innovant d'expérimentation, applicable notamment aux traitements de souveraineté, pourrait, à cette occasion, constituer une réelle avancée pour les autorités de police et de gendarmerie, et constituer en même temps un gage de transparence pour une opinion publique légitimement soucieuse du respect des libertés individuelles et du secret de la vie privée.

[98] Point 8 de l'annexe 3.
[99] 6a. de l'article 29 et annexe 3.
[100] Cf. notamment le point 7 de l'exposé des motifs et 48.a et 48b.
[101] Conseil d'Etat *« Intelligence artificielle et action publique : construire la confiance, servir la performance »* 31 août 2022, notamment p.84.

Fabienne DUTHE
Commissaire générale,
inspection générale de la
police nationale

Pascal GIRAULT
Inspecteur général
de l'administration

Jean-Marc TEISSIER
Colonel, inspection générale
de la gendarmerie nationale



Daniel MONTIEL
Commissaire général,
inspection générale de la
police nationale

Anne CORNET
Inspectrice générale
de l'administration

Christophe BAUDRY
Colonel, inspection générale de
la gendarmerie nationale

ANNEXES

Annexe n° 1 : Lettre de mission

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Le Préfet,

Directeur du Cabinet

Monsieur Michel ROUZEAU
Chef du service de l'inspection générale de l'administration

Madame Agnès THIBAULT-LECUIVRE
Cheffe de l'inspection générale de la police nationale

Monsieur Jean-Michel GENTIL
Chef de l'inspection générale de la gendarmerie nationale

Paris, 24/11/2023

Objet : Mission inter-inspections relative à l'usage de logiciels d'analyse vidéo par les services de la police et la gendarmerie nationales

Le 14 novembre 2023, un média en ligne publiait un article faisant état de l'utilisation par la police nationale et par une centaine de polices municipales du logiciel Briefcam, et en particulier de sa fonctionnalité de reconnaissance faciale appliquée à des images issues de vidéoprotection. Selon l'article, cette utilisation aurait permis le suivi massif de personnes à distance, y compris en temps réel et dans l'espace public, en dehors du cadre légal en vigueur.

Les services d'investigation du ministère de l'Intérieur et des Outre-mer ont un besoin croissant d'analyse de vidéos pour améliorer l'identification de mis en cause et faciliter l'élucidation. Ceci est renforcé par la hausse des dispositifs vidéo installés par les communes, les personnes morales et les particuliers, fournissant de nouveaux éléments aux enquêteurs. Par ailleurs, la systématisation de la production de preuve par l'image réduit les situations de contestation, raccourcit les délais d'enquête et facilite le prononcé de peines par l'autorité judiciaire.

Si l'utilisation de logiciels d'analyse vidéo par les services d'investigation n'est pas illégale en soi, elle doit effectivement s'inscrire dans un cadre juridique précis. Un certain nombre de garanties pour les libertés publiques ont ainsi été fixées par le législateur.

Le régime juridique des logiciels de rapprochement judiciaire (LRJ) en particulier est défini à l'article 230-20 du code de procédure pénale. Ces outils ne peuvent être utilisés que sous l'autorité du magistrat et uniquement par des agents individuellement habilités. Ils ne peuvent avoir pour finalité que de « faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs », ainsi que « l'exploitation et le rapprochement d'informations sur les modes opératoires réunies au cours des enquêtes ou procédures ».

Ces dispositions ont fait l'objet d'un acte réglementaire unique - « Acte cadre » (Décret n° 2012-687 du 7 mai 2012) qui encadre l'ensemble des traitements présentant des caractéristiques similaires et qui ne nécessitent pas l'adoption d'actes réglementaires spécifiques. L'autorisation de mise en œuvre de ces traitements nécessite donc uniquement l'envoi d'un engagement de conformité à la CNIL, accompagné d'un dossier de présentation du logiciel. Selon l'analyse menée par la DLPAJ en janvier 2023, ce décret ne prévoyant pas explicitement le recours à la reconnaissance faciale, cette fonctionnalité n'est en revanche pas autorisée en l'état du droit.

Place Beauvau
75800 PARIS Cedex 08
Standard : 01 49 27 49 27 – 01 40 07 60 60
Adresse internet : www.interieur.gouv.fr

Aussi, je vous demande de bien vouloir diligenter une mission inter-inspections sur l'utilisation de logiciels d'analyse vidéo par les services de la police et la gendarmerie nationales. Sans se limiter au seul logiciel Briefcam, vous me rendrez compte :

- Des cas d'utilisation éventuels de ces logiciels au sein des services d'investigation. En particulier, vous dresserez la liste exhaustive des unités ayant recours ou ayant eu recours à de tel outils, ainsi que la nature des outils en question. Vous évaluerez aussi précisément que possible leur degré d'utilisation (nombre d'agent habilités, fonctionnalités les plus utilisées, date de début de l'utilisation etc.) ;
- Du respect du cadre légal en vigueur dans l'utilisation de ces logiciels. En particulier, vous vous assurerez :
    - Que les fonctionnalités de reconnaissance faciale ne sont pas mises en œuvre ;
    - Que ces logiciels ne sont utilisés que dans un cadre judiciaire, sous l'autorité des magistrats.
- De toutes propositions visant à améliorer les mécanismes de contrôle interne dans la mise en œuvre de dispositifs technologiques expérimentaux, afin de prévenir leur utilisation éventuellement litigieuse, sans proscrire pour autant l'esprit d'innovation qui doit prévaloir au sein des forces de l'ordre.

Vos travaux me seront remis dans un délai de trois mois à compter de la réception de la présente lettre de mission.

Bien cordialement,

Alexandre BRUGÈRE

Annexe n° 2 : Liste des personnes rencontrées

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

CABINET

- Marie GAUTIER-MELLERAY, directrice adjointe
- Tristan FULCHIRON, conseiller transformation numérique
- François-Xavier LESUEUR, conseiller gendarmerie (mission opérationnelle de sécurité et de défense)
- Pierre-Edouard COLLIEX, conseiller police (mission opérationnelle de sécurité et de défense)

DIRECTION GENERALE DE LA GENDARMERIE NATIONALE

- Christian RODRIGUEZ, directeur général
- Thibaud LAGRANGE, chargé de mission auprès du directeur général
- Marc BOGET, directeur de la stratégie digitale et technologique
- Philippe CAUSSE, commandant en second du pôle judiciaire de la gendarmerie nationale
- Adrien VERON, chef du bureau stratégie innovation (direction des opérations et de l'emploi - DOE -, sous-direction de la police judiciaire)
- Renald BOISMOREAU, chef du service central de renseignement criminel - SCRC -
- Frédérick REHAULT, chef de la division des fichiers - SCRC
- Benjamin GRAS, enquêteur DIEAF/DO - SCRC
- Olivier SCHMIT, chef du département investigation véhicules - SCRC
- Florent REMUSATI, officier concepteur, bureau stratégie innovation (DOE, sous-direction de la police judiciaire)
- Christophe MENEAU, chef du pôle juridique et judiciaire (cabinet DGGN)
- Frédéric TARDIF, conseiller juridique et judiciaire DOE
- Marie TONANNY, cheffe du bureau administration de la donnée - service de la transformation

DIRECTION GENERALE DE LA POLICE NATIONALE

- Frédéric VEAUX, directeur général
- Alex GADRE, conseiller juridique (cabinet DGPN)
- Adeline CHAMPAGNAT, conseillère technologies et numérique (cabinet DGPN)

DIRECTION NATIONALE DE LA POLICE JUDICIAIRE

- Christian SAINTE, directeur national
- Aymeric SAUDUBRAY, directeur national adjoint
- Christine DUFAU, cheffe du département des technologies appliquées à l'investigation (D@ta-i)
- Marie-Catherine SAVREUX-LECLERCQ, cheffe de projet maîtrise d'ouvrage Système V
- Stéphane RUELLAN, responsable du pôle assistance et pilotage de projets

DIRECTION NATIONALE DE LA SECURITE PUBLIQUE

- Virginie BRUNNER, directrice
- Elisabeth FOUILLOUX, cheffe du département numérique
- Alexandre BONNEVILLE, sous-directeur de la sécurité du quotidien et des partenariats

DIRECTION NATIONALE DE LA POLICE AUX FRONTIERES

- Valérie MINNE, directrice nationale
- Véronique LEFAURE, cheffe du département du numérique

AGENCE DU NUMERIQUE DES FORCES DE SECURITE INTERIEURE

- Frédéric AUBANEL, directeur
- Régis LAPORTE, directeur adjointe

DIRECTION NATIONALE DU RENSEIGNEMENT TERRITORIAL

- Alain BRAUD, directeur adjoint

PREFECTURE DE POLICE DE PARIS

DIRECTION DE LA SECURITE DE PROXIMITE DE L'AGGLOMERATION PARISIENNE

- Isabelle TOMATIS, directrice
- Jean-Paul PECQUET, directeur adjoint
- Jean-Luc MERCIER, chef d'état-major
- Gilles PETITCOLIN, état-major, chef de la division de la coordination judiciaire (DCJ)
- Olivier JEANNES, chef de l'unité d'assistance technique (DCJ)

DIRECTION DE LA POLICE JUDICIAIRE

- Marc THORAVAL, directeur adjoint

DIRECTION DES LIBERTES PUBLIQUES ET DES AFFAIRES JURIDIQUES

- Pascale LEGLISE, directrice
- Léa QUIAU, cheffe du bureau du droit des données et des nouvelles technologies

DELEGUE MINISTERIEL A LA PROTECTION DES DONNEES

- Fabrice MATTATIA, délégué ministériel

DIRECTION DES ENTREPRISES ET PARTENARIATS DE SECURITE ET DES ARMES

- Julie MERCIER, directrice
- Elisabeth SELLOS-CARTEL, adjointe en charge de la mission vidéoprotection

DIRECTION ZONALE SUD-EST DE LA POLICE NATIONALE

- Béatrice BRUN, directrice zonale
- Nadine LE CALONNEC, cheffe du service zonale de sécurité publique
- Damien DELABY, chef du service zonal de police judiciaire
- Matthieu BERNIER, directeur interdépartemental adjoint du Rhône

SERVICE NATIONAL DE LA POLICE SCIENTIFIQUE

- Eric ANGELINO, chef du service
- Denis PERRAUD, chef du laboratoire central de criminalistique numérique
- Anthony HAPIAK, chef du bureau de la doctrine et de la réglementation
- Christopher ETIENNE, analyste téléphonie

SERVICE INTERDEPARTEMENTAL DE LA POLICE JUDICIAIRE DE SEINE-ET-MARNE

- François MALHERBE, chef du service
- Gilles CANTENOT, enquêteur (unité d'aide à l'enquête)
- Stéphane LENOIR, enquêteur stupéfiants
- Jean-François DESCAMPS, opérateur SIAT 78

SECTION DE RECHERCHE DE PARIS (GENDARMERIE NATIONALE)

- Patrick PEGEOT, commandant de la section de recherche
- Yakout BOUDALI, adjointe division atteintes aux personnes
- Deborah DURAND, enquêtrice
- Cindy ROGUET, enquêtrice

- Thomas GUERAUD, adjoint au commandant de la division atteintes aux biens
- Christophe CERTAIN, chef de la division atteinte aux biens
- Antoine AURIAULT, enquêteur

DIRECTION INTERDEPARTEMENTALE DE LA POLICE JUDICIAIRE DE VERSAILLES

- Patricia DOYEN, cheffe du SIAT 78
- Frédéric BAHLER, adjoint à la cheffe du SIAT 78
- Geneviève HOFFMANN, cheffe de l'antenne OFAC 78
- Maxime DE POURCK, chef de la section criminalistique numérique
- Steeve THIRIOT, adjoint au chef du service départemental d'assistance technique

DIRECTION INTERDEPARTEMENTALE DE LA POLICE JUDICIAIRE DE TOULOUSE

- Patrick LEONARD, chef du service interdépartemental de police judiciaire
- Marion AUDIGIER, directrice interdépartementale de la police nationale adjointe
- Jean-François LESPES, chef du bureau de coordination opérationnelle et de synthèse de la division du pilotage opérationnel du service interdépartemental de police
- Sandrine COLLET, cheffe de la brigade des atteintes aux biens de la division de la criminalité territoriale
- Romain FROMENT, enquêteur de la brigade des atteintes aux biens de la division de la criminalité territoriale

CONSEIL D'ETAT

- Christian VIGOUROUX, conseiller d'Etat honoraire
- Florian ROUSSEL, maître des requêtes
- Thierry THUOT, président de la section de l'intérieur
- Christine MAUGÜE, présidente adjointe de la section de l'intérieur
- Didier CHAUVAUX, président adjoint de la section de l'intérieur
- Michel DELPUECH, conseiller d'Etat

CNIL

- Louis DUTHEILLET de LAMOTHE, secrétaire général
- Benjamin VIALLE, chef du service des contrôles RH, santé et affaires publiques, direction de la protection des droits et des sanctions
- Thomas DAUTIEU, directeur de l'accompagnement juridique
- Sarah ARTOLA, service des affaires régaliennes et des collectivités territoriales, direction de l'accompagnement juridique

SOCIETE M2M FACTORY

- Jérémie CARON, directeur général
- Laurent SUFFYS, responsable production

Annexe n° 3 : Présentation et doctrine d'emploi de *Système V*

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

POLICE
NATIONALE

Doctrine d'emploi du traitement Système V

Système V est un traitement prévu à l'usage des enquêteurs de la police nationale et de la gendarmerie nationale. En cours de développement depuis avril 2020, l'application répond aux besoins opérationnels d'analyse rapide d'importants volumes d'images vidéo traitées par ces enquêteurs.

L'application Système V permet aux services chargés d'enquêtes judiciaires d'analyser et d'exploiter les sources vidéo faisant apparaître une situation ou un fait susceptible de concourir à la résolution de ces enquêtes et collectées dans ce cadre, au sein d'un même outil de travail collaboratif.

L'utilisation de ce nouveau logiciel est indissociable d'une application stricte des règles de sécurité conformes à la politique de sécurité des systèmes d'information de la police nationale (PSSI PN), ainsi qu'aux dispositions des règlements européens n°2016/679 et n°2016/680 telles que transposées dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

I. Cadre juridique d'utilisation

1. Champ d'utilisation

Système V, qui fait l'objet d'un engagement de conformité au 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 (décret I.R.I), répond à deux finalités complémentaires :

- la facilitation du traitement des fichiers vidéo collectés dans le cadre d'enquêtes déterminées aux fins de leur résolution par les enquêteurs, en permettant une détection plus rapide des éléments de preuve pouvant être versés à l'enquête ;
- l'optimisation de l'organisation des services d'enquête, en permettant une continuité dans le suivi et l'avancement de l'analyse par les enquêteurs et une réduction du temps consacré par ces derniers au visionnage des fichiers vidéo.

L'application Système V est utilisée dans le cadre d'une enquête judiciaire déterminée. Elle peut être mise en œuvre pour toutes les infractions. Seul le domaine contraventionnel est exclu du cadre de son utilisation. L'enquêteur responsable du dossier peut importer les fichiers vidéo récupérés lors des investigations dans Système V, et peut alors y lire les vidéos (comme sur un lecteur vidéo classique), ou lancer une recherche faisant intervenir l'intelligence artificielle pour détecter une silhouette, un véhicule, une couleur ou un mouvement.

La mise en œuvre de ce logiciel est soumise à l'autorisation du magistrat compétent. En matière d'enquête de flagrance, l'autorisation est réputée acquise, sauf décision contraire du procureur de la République. De plus, la mise en œuvre de Système V fait l'objet d'une mention en procédure.

Place Beauvau
75800 PARIS Cedex 08
Standard : 01 49 27 49 27 – 01 40 07 60 60
Adresse internet : www.police-nationale.interieur.gouv.fr

Dès la clôture de l'enquête, l'exploitation des donnés implique l'établissement d'un rapport qui sera joint à la procédure.

Système V est divisé en autant de bases locales qu'il existe de services utilisateurs. Chaque base est indépendante, l'accès à l'application se faisant grâce à une station dédiée reliée au réseau local du service et depuis les postes de bureautique reliés à ce même réseau. Les utilisateurs n'ont donc accès qu'aux données produites localement par leur service, sous réserve des habilitations qui leur ont été accordées par leur chef de service. Aucun tiers ne peut accéder aux données, et aucun export de celles-ci n'est prévu.

Système V peut être utilisé en mode nomade (télétravail, déplacements) sous autorisation et encadrement du chef de service.

2. Accès aux données

L'application est accessible par authentification forte, par carte agent et code pin. Dans la version actuelle de l'outil, elle coexiste avec un mode d'authentification alternatif (par login/mot de passe), qui restera possible en cas d'obstacle ponctuel à une authentification par carte agent.

Les authentifiants permettant l'administration de Système V doivent être remis au RSSI de chaque entité territoriale pour être placés au coffre (celui du RSSI ou, à défaut, celui du chef de service). Toute modification de ces authentifiants doit être communiquée au RSSI.

L'usage privilégié est d'importer les vidéos depuis le poste de travail de l'agent. Il est autorisé de les importer à partir du serveur si et seulement si un « crash » du réseau rend l'utilisation classique de Système V inopérante, et avec un compte sans privilèges.

Une fois connecté, l'utilisateur peut accéder aux données de Système V en fonction du profil qui lui aura été attribué :

- l'enquêteur alimente et exploite effectivement le logiciel, dans le cadre des dossiers d'enquête auxquels il a accès (ceux-ci étant déterminés par le chef de service ou d'unité). Il peut importer, visionner, analyser et commenter les fichiers vidéo, générer les rapports correspondants et clôturer les dossiers d'enquête auxquels il participe ;
- l'administrateur dispose des mêmes droits que l'enquêteur, mais assure également la création des comptes et des groupes d'enquête, la gestion des habilitations des agents de son service et voit l'ensemble des dossiers du service créés dans Système V.

Quel que soit le profil utilisé, l'ensemble de ces opérations (connexion, import, recherche, suppression, rapport) fera l'objet de données de traçabilité, permettant ainsi l'analyse des journaux, la détection de comportements anormaux sur le système d'information et la surveillance de ses flux d'entrée et de sortie.

Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit. L'utilisateur doit être informé de l'existence de l'ensemble de ces opérations de gestion, de leurs finalités et limites.

II. Gestion des données

Le droit positif impose à tout traitement collectant des données à caractère personnel des garanties assurant une minimisation des données collectées de cette nature, et un contrôle de la qualité de celles qui auront été collectées dans le cadre des finalités du traitement. Dans le prolongement de ces mesures, un soin particulier doit également être apporté aux mécanismes d'effacement des données.

1. Minimisation des données

S'agissant des fichiers vidéo importés dans Système V : dans le seul cadre des finalités déterminées pour le traitement, ils ne doivent correspondre qu'à ceux qui seraient visionnés par un enquêteur dans le cadre de la résolution d'une enquête judiciaire à des fins de recherche d'éléments de preuve. Chaque vidéo importée dans l'application ne peut l'être que **dans le cadre d'une enquête précise et pour des circonstances déterminées**.

S'agissant des données saisies par l'enquêteur dans Système V : deux zones de champs libres existent dans Système V et doivent faire l'objet d'une attention particulière :

- Les champs « nom du dossier » et « lieu des faits » ; dans la limite de 32 caractères, l'enquêteur doit nommer le dossier lors de la création d'un nouveau dossier d'enquête dans l'application. Le nom du dossier doit correspondre au nom donné à l'enquête, en évitant, dans la mesure du possible, de citer le nom de la victime ou du MEC. Le type d'enquête ainsi que le lieu sont donc à privilégier dans le nommage du dossier (*exemple* : « *VMA place de l'Etoile* »).
- Les champs « MAN » (marqueur manuel) et « IA » (intelligence artificielle) limités à 5 500 caractères :
  - L'enquêteur peut y décrire objectivement les éléments visibles sur les images vidéo ou audibles sur le son du fichier dès lors que ceux-ci sont pertinents aux fins de la résolution de l'enquête judiciaire concernée. L'enquêteur se contente alors d'**éléments exclusivement factuels, ne pouvant donner lieu à interprétation** (*exemple* : « *arrivée d'un individu correspondant au signalement fait par la victime à 10h28* »). Ces données permettent de contextualiser et de bien comprendre la nature de l'événement étudié, et pourront être intégrés au rapport généré depuis l'application. Le référentiel Bauer[1] peut être utilisé, si cela est nécessaire, dans la description des personnes concernées.
  - L'enquêteur peut également y saisir des notes de travail (*exemple* : « *analyse suspendue à 10h30* ») pour permettre le suivi et la continuité de son travail en cas de relais avec un autre enquêteur. Ces notes de travail ne sont pas intégrées au rapport généré depuis l'application.

2. Garanties pour la qualité des données

Les agents habilités à l'utilisation de Système V ont à disposition divers supports de formation :

- tutoriels vidéo pour chaque module de l'application ;
- manuel utilisateur sous forme de fiches ;
- mallette pédagogique relative à l'administration technique (Linux) de l'application[2].

Le chef d'unité ou de service doit opérer, dès lors qu'il consulte un fichier vidéo ou accède aux champs libres de l'application, un **contrôle de l'opportunité, de la cohérence et de l'exactitude des données** traitées par Système V. Il veille aussi à ce que tous les champs nécessaires soient bien renseignés et complétés par les enquêteurs habilités sur chaque dossier d'enquête. Le contrôle des saisies par le supérieur hiérarchique peut être périodique et aléatoire.

Il pourra à cette occasion effacer de l'application tout fichier vidéo dont l'exploitation ne correspondrait pas au cadre de l'enquête concernée, mais aussi vérifier que les systèmes d'horodatage et les droits de chaque utilisateur dans l'application sont à jour. Dans le cas où des incohérences ou des erreurs

1 Déterminant onze types : caucasien, méditerranéen, moyen-oriental, maghrébin, asiatique/eurasien, amérindien, indo-pakistanais, métis-mulâtre, africain/antillais, polynésien et mélanésien (dont canaque).

2 Un projet de e-formation est également en cours (au stade de la rédaction de fiches par la maîtrise d'œuvre).

Place Beauvau
75800 PARIS Cedex 08
Standard : 01 49 27 49 27 – 01 40 07 60 60
Adresse internet : www.police-nationale.interieur.gouv.fr

seraient détectées, celles-ci devront immédiatement être corrigées, et des instructions devront être données afin d'éviter leur réitération.

3. Effacement des données

Dans la version actuelle de l'outil, l'effacement des données se fait manuellement par un agent habilité (enquêteur ou administrateur), dans deux cas :

- De façon anticipée à la clôture de l'enquête, lorsque celle-ci a été élucidée et qu'il n'existe aucune probabilité de poursuite des investigations, ou qu'elle se poursuive dans un autre cadre procédural. En toute hypothèse, cette décision devra faire l'objet d'un contrôle d'opportunité par le supérieur hiérarchique ;
- Au plus tard à l'issue de la durée de conservation légale des données, à savoir 3 ans à compter de l'enregistrement (import ou saisie) de données dans l'application.

N.B. : dans la continuité des mesures visant à garantir la **qualité** et la **minimisation** des données traitées par Système V, chaque agent habilité devra également s'assurer du bon effacement de tout commentaire ou fichier vidéo qui ne serait pas exploitable au sein du dossier d'enquête, pour des raisons techniques (*exemple :* mauvaise qualité de l'image) ou opérationnelles (*exemple :* mauvais angle de prise de vue, empêchant tout apport d'élément pertinent).

III. Sécurité du traitement

1. Revues d'habilitation

Des revues d'habilitation et des autorisations d'accès doivent être menées tous les ans par le chef d'unité ou de service avec l'appui de l'acteur SSI local. À cette occasion, ce dernier vérifie l'exactitude des données relatives aux utilisateurs de Système V relevant de son service et des fiches d'habilitation individuelles leur étant associées, le bon niveau d'accès et de droits de chacun d'eux, ainsi que la bonne suppression des accès obsolètes (*exemple :* utilisateurs qui auraient quitté le service dont il est responsable). La fiche d'habilitation individuelle sera conservée au dossier individuel de l'agent.

Un processus formalisé de gestion des arrivées et des départs est également mis en œuvre, garantissant ainsi la légitimité des accès accordés. Cette procédure formalisée, qui recouvre les arrivées, mutations et départs des agents, couvre la gestion et la révocation des comptes et des droits d'accès aux SI, mais aussi la gestion du contrôle d'accès aux locaux.

2. Protection des données

Les flux d'administration sont protégés par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'agence nationale de sécurité des systèmes d'information (ANSSI). L'administration doit être opérée sur la machine Système V par l'administrateur technique local :

- par un protocole de communication sécurisé (via une prise en main distante) par la Section opérationnelle de lutte contre la cybercriminalité (SOLC) pour la gendarmerie nationale ;
- par le même procédé par le Bureau départemental des systèmes d'information et des transmissions (BDSIT) pour la police nationale.

Afin d'assurer la sécurité physique des équipements, l'accès aux locaux est sécurisé par un contrôle des cartes professionnelles (manuel ou automatisé) dans les zones non destinées à recevoir le public. L'enregistrement des visiteurs se fait au bureau d'accueil avec les coordonnées et le nom du

responsable accompagnateur, la date et l'heure de la visite, le lieu visité et l'heure de départ. Tout visiteur est en permanence accompagné.

Il conviendra de privilégier la salle serveur pour l'emplacement du serveur Système V, dont l'accès devra être sécurisé par le moyen le plus approprié en fonction de la configuration des locaux.

Le RSSI effectue des mesures de sensibilisation à la SSI envers les utilisateurs et les administrateurs techniques.

3. Sécurisation des documents papier

Dans l'attente du déploiement de la procédure pénale numérique, les exports générés par l'application Système V peuvent être imprimés. Ces documents ne peuvent être conservés en commissariat que dans le cas où ils sont annexés et versés à la procédure.

Dès lors que les évolutions de Système V le prévoiront, ces impressions devront faire l'objet d'un niveau de protection équivalent à celui des autres documents papier produits dans les services de police (respect du secret de l'enquête prévu par l'article 11 du Code de procédure pénale). Les impressions papier ne devront pas être laissées à la vue des agents n'ayant pas à en connaître, ni à celle du public. À la fin de leur service, les agents à l'origine des impressions devront les soustraire à la vue de tiers et les mettre en sécurité. Alors, la fermeture à clé des armoires où seront classés ces documents est obligatoire.

Place Beauvau
75800 PARIS Cedex 08
Standard : 01 49 27 49 27 – 01 40 07 60 60
Adresse internet : www.police-nationale.interieur.gouv.fr

Annexe n° 4 : L'usage de l'analyse vidéo : comparaisons internationales

Partie I : Éléments de comparaison des pratiques

I – Pays européens

ALLEMAGNE

A – Au niveau fédéral

Quels sont les logiciels utilisés et leurs fonctionnalités (sélection de passages comportant des items intéressants de type « dérushage », analyse comportementale, reconnaissance faciale…) ?

La Police fédérale a testé pendant dix-huit mois un logiciel d'analyse vidéo semi-automatique en matière de lutte contre la criminalité (poursuite pénale) et le pérennisera probablement au début de l'année 2024. Il s'agit du système logiciel « Investigator » du fournisseur Digivod. Il permet de lire et d'analyser de grandes quantités de données images et vidéos ainsi que d'effectuer une recherche ciblée dans le stock de données. Il est par exemple possible de rechercher des véhicules, des couleurs, des personnes, l'âge et le sexe apparents, des objets (valises, sacs à dos, etc.), du texte et des logos. Cette liste n'est pas exhaustive. Comme il s'agit d'un système logiciel extensible, d'autres fonctionnalités, appelées détecteurs, peuvent être développées et intégrées par le fabricant.

L'application dispose de la reconnaissance faciale. L'origine des données multimédia ne joue aucun rôle dans leur évaluation par le logiciel, pour autant que le format des données soit lisible. Le système prend en charge un grand nombre de formats vidéo courants, mais aussi propriétaires. L'intégration de nouveaux formats vidéo par le fabricant est également possible.

Quel est le cadre juridique de leur utilisation (judiciaire, administratif…) ?

L'analyse vidéo semi-automatisée est utilisée de manière ciblée par la Police fédérale afin d'obtenir des preuves à charge et à décharge dans le cadre de procédures pénales déterminées et graves, susceptibles d'entrer dans le champ d'application de l'article §100a du Code de procédure pénale[1], dites « infractions cataloguées ».
Une utilisation préventive du logiciel n'est actuellement pas autorisée.

Quelles sont les entités qui les utilisent (forces de sécurité étatiques, régionales, municipales, autres collectivités territoriales…) ?

Le logiciel sera mis à disposition dans deux services sélectionnés de la Police fédérale et sera utilisé localement en soutien aux enquêtes. Tous les services de la Police fédérale qui en auront besoin pourront recourir aux capacités du système. Pour ce faire, les données à analyser seront transmises à l'un de ces deux services, où elles seront lues, évaluées et les résultats communiqués aux demandeurs.

Quels sont les contrôles dont ces logiciels font l'objet (sont-ils soumis à validation préalable ? Selon quelles modalités ? Des personnes hors cadre institutionnel ont-elles accès à leurs caractéristiques, notamment des personnes issues de la « société civile » ?

Le logiciel « Investigator » a été testé dans le cadre d'un essai de dix-huit mois afin de déterminer s'il était adapté à l'accomplissement des tâches de la Police fédérale. L'examen a été effectué sur la base de critères policiers, techniques et juridiques. Il a été constaté que la valeur ajoutée en matière de police pour lutter contre la criminalité était considérable. Sur le plan technique, la performance et la stabilité du système ont été jugées suffisantes pour son utilisation. Tous les accès au système se font exclusivement par le personnel autorisé de la Police fédérale au moyen d'un identifiant personnel. Le système consigne toutes les activités d'évaluation et les attribue à l'agent concerné. Un accès de l'extérieur, par Internet, n'est pas possible, car les systèmes fonctionnent chacun dans leur propre réseau, indépendant du reste de l'infrastructure réseau de la Police fédérale.

Des polémiques ou des contestations ont-elles eu lieu ou sont-elles en cours sur ces logiciels et leurs fonctionnalités, respectivement dans l'espace public ou lors de procès ? De quelle manière sont ou ont-elles gérées par les autorités ? Quelles sont leurs conséquences ?

Étant donné que le logiciel a été testé, son utilisation n'a pas encore fait l'objet de procédures judiciaires. Il n'y a pas non plus eu de débat public jusqu'à présent. Comme le logiciel n'est utilisé qu'en matière de poursuite pénale et non de manière préventive, le ministère fédéral de l'Intérieur et du Territoire (BMI) s'attend à un éventuel débat public nettement plus modéré que les logiciels similaires en matière de prévention de la menace.

1 Cet article liste les infractions susceptibles de justifier des mesures de surveillance des télécommunications. Des infractions sont listées, couvrant tant le droit pénal général, la criminalité organisée ou certaines infractions en matière de droit des étrangers. Plusieurs infractions sportives sont également visées.

Commentaires : *ces éléments concernent la Police fédérale. Pour mémoire, la compétence policière appartient constitutionnellement aux entités fédérées, les Länder.*

Un projet pilote de « vidéosurveillance intelligente » a également été lancé à Mannheim fin 2018. Depuis juillet 2023, elle est également utilisée dans le quartier de St. Georg à Hambourg où la Hansaplatz est équipée à titre expérimental pendant trois mois. Il ne fonctionne toutefois pas avec une reconnaissance faciale mais enregistre certains modèles de comportement considérés comme typiques d'une action criminelle en préparation. Les enregistrements vidéo réalisés par les caméras sont analysés par un logiciel développé par l'Institut Fraunhofer pour l'optronique, la technique des systèmes et l'évaluation des images (IOSB).

B – Au niveau des *Landër*

Pour l'usage de la reconnaissance faciale, le Land de Saxe est a développé un outil très performant, le projet **Perls** : prise de clichés photos des conducteurs et passagers avant de véhicules en mouvement, y compris de nuit et avec la pluie, d'une qualité telle qu'elle permet ensuite la comparaison avec une base de données (reconnaissance faciale). Le détail de leur contribution est en attente.

Cette entité fédérée a été sollicitée par le SSI pour davantage de détails ont été, mais avec les *Landër*, les délais sont souvent bien plus longs qu'avec les structures de niveau fédéral.

AUTRICHE

Les autorités autrichiennes n'ont pas encore répondu à la sollicitation du SSI. Leur retour vous parviendra à réception.

BELGIQUE

Les autorités belges n'ont pas encore répondu à la sollicitation du SSI. Leur retour vous parviendra à réception.

BULGARIE

Les logiciels utilisés et leurs fonctionnalités (sélection de passages comportant des items intéressants, analyse comportementale, reconnaissance faciale…)

Pour l'analyse intelligente des informations vidéo, les services bulgares utilisent le logiciel "Protect" de la société BriefCam, l'un des principaux fournisseurs en matière de technologie pour l'examen et la recherche rapides de vidéos, l'alerte en temps réel et l'analyse quantitative de vidéos.

La vidéo brute est transformée en une source d'information intelligente et exploitable. Le logiciel facilite le travail du personnel d'exploitation en réduisant considérablement le temps nécessaire à l'examen du contenu vidéo et à l'optimisation des opérations. La combinaison de la vision par ordinateur et des technologies de Deep Learning et de Video Synopsis permet aux opérateurs d'examiner des heures de séquences en quelques minutes seulement et d'identifier rapidement les personnes et les objets d'intérêt. Voici quelques-unes des options permettant de rechercher et de filtrer rapidement les objets et les événements :
- Filtrage temporel ;
- Filtrage par classe - personnes (hommes, femmes, enfants) ; véhicules à deux roues - bicyclettes, motos ; autres véhicules - voitures, bus, camionnettes, trains, avions, bateaux ;
- Filtrage par attributs de classe - sacs (sacs à dos, sacs à main) ; avec/sans chapeau ; vêtements (manches courtes, manches longues, sans manches)
- Filtrage par couleur, etc.

Le cadre juridique de leur utilisation

Le système a été mis en service par un décret ministériel de 2019 sur la base de la loi sur le ministère de l'Intérieur et son exploitation se fait conformément à des règles internes spécifiques approuvées.
Les fondements normatifs de l'utilisation des systèmes de vidéosurveillance et des dispositifs d'enregistrement vidéo par les forces de l'ordre sont contenus dans la loi sur le ministère de l'Intérieur (article 101, paragraphe 1), la loi sur la circulation routière (article 165, paragraphe 2, point 7), la loi sur la protection de l'ordre public lors des manifestations sportives (article 29), ainsi que dans plusieurs instructions détaillant les règles relatives à l'exercice des fonctions spécifiques pertinentes des autorités compétentes.

Les entités qui les utilisent (forces de sécurité étatiques, régionales, municipales, autres collectivités territoriales…)

Le système est utilisé par les officiers de police pour enquêter et trouver rapidement des informations pour faciliter le travail opérationnel.

Les contrôles dont ces logiciels font l'objet (sont-ils soumis à validation préalable ? Selon quelles modalités ? Des personnes hors cadre institutionnel ont-elles accès à leurs caractéristiques, notamment des personnes issues de la "société civile" ?

L'accès au système est accordé à certains employés du ministère de l'Intérieur, au centre de surveillance du département de la sécurité de la municipalité de Sofia et au centre de surveillance de la DANS (équivalent de la DGSI). L'accès de la municipalité de Sofia et de la DANS est régi par un accord de coopération tripartite qui entrera en vigueur en 2022.

Si des polémiques ou des contestations ont eu lieu ou sont en cours sur ces logiciels et leurs fonctionnalités, respectivement dans l'espace public ou lors de procès, et la façon dont elles ont été/sont gérées par les autorités, leurs conséquences…

Le système utilisé jusqu'à présent n'a fait l'objet d'aucune controverse ou protestation.

CHYPRE

La vidéosurveillance de l'espace public n'est pas autorisée à Chypre, qui possède une des législations les plus protectrices de l'UE. La mise en place d'un logiciel d'analyse de masse (même si elle serait particulièrement appréciée par les autorités policières) n'est donc pas à l'ordre du jour.

CROATIE

Les forces de l'ordre croates n'utilisent pas le logiciel « Briefcam », ni autre solution logicielle, et n'ont donc pas de retour d'expérience.

ESPAGNE

Les autorités espagnoles n'ont pas encore répondu à la sollicitation du SSI. Leur retour vous parviendra à réception.

GRÈCE

La Police grecque ne dispose pas de logiciel d'analyse vidéo de masse.

HONGRIE

1. *Quel logiciel utilisez-vous et quelles sont ses fonctions* ? (sélection de passages contenant des éléments d'intérêt, analyse comportementale, reconnaissance faciale, etc.)

Au sein des forces de police hongroise, la Préfecture de police de Budapest utilise un logiciel de reconnaissance faciale de type NEC NEOFACE à l'occasion des grands événements, visant à contrôler les entrées par des points d'accès définis. L'objectif vise ainsi l'identification de personnes à partir d'une base de données. Le logiciel ne réalise pas d'analyse comportementale.

En outre, lors des événements de masse, sportifs ou culturels, la police d'intervention (DGPN) met en place un dispositif de surveillance vidéo des lieux publics sur les sites concernés afin de prévenir les troubles ou aider à leur répression. Les images enregistrées en temps réel peuvent également être transmises directement dans un centre de commandement.
Lors des enregistrements, aucun logiciel d'analyse vidéo ou de reconnaissance faciale n'est utilisé. En cas d'infraction, les enregistrements sont transmis aux services judiciaires pour prise en compte et traitement.

2. *Quel cadre juridique définit cette utilisation* ?

Aux termes de la loi CLXXXVIII. de 2015 sur le système de reconnaissance faciale (dite « loi de l'image faciale » - traduction littérale) et du décret gouvernemental 350.2016. (XI.18.), le Centre national de recherche et d'expertise est l'organe chargé de la gestion du système de reconnaissance faciale.
La Police a le droit d'utiliser le service de reconnaissance faciale en respectant les paragraphes 2,4,8,10, 11 de la loi sur l'image faciale. L'utilisation d'un logiciel d'analyse faciale lors d'une procédure pénale par les services d'enquêtes est possible en vertu de la loi XC. De l'an 2017.

3. *Quelles sont les entités équipées* ?
Les services ayant le droit d'utiliser ces logiciels sont les suivants :

- Les services de Police
- Le bureau du Procureur
- Le centre anti-terroriste
- Le service pénitentiaire
- L'organe chargé de la délivrance des pièces d'identité

- Les services de sécurité nationale
- Les gardes parlementaires
- Le bureau chargé de la protection de la Constitution
- Le bureau de l'Information
- Le service militaire de sécurité nationale
- Le service de la protection des témoins

Le paragraphe 2 liste des services ayant droit à l'utilisation (Police, service chargé de la procédure préliminaire, service d'enquête, le bureau du procureur, service de prévention et de renseignement criminel).

Le paragraphe 4 est relatif à l'utilisation des logiciels de reconnaissance faciale à des fins d'identification des personnes recherchées / disparues.

Le paragraphe 8 est relatif à l'utilisation des logiciels de reconnaissance faciale par des forces de police / centre anti-terroriste / gardes parlementaires à des fins de protection rapprochée de hautes personnalités (contrôle d'identité, identification de personnes inconnues).

Le paragraphe 10 concerne l'utilisation des logiciels de reconnaissance faciale à des fins d'identification et de droit à l'entrée dans les bâtiments importants (Police, administrations gouvernementales).

Le paragraphe 11 est sur l'utilisation des logiciels de reconnaissance faciale à la demande des autorités étrangères dans le cadre d'une entraide judiciaire pour analyser les auteurs présumés sur les images fixes ou animées ou sur les dessins. Les services autorisés à l'utilisation sont la DGPN, le NEBEK (Centre de coopération pénale internationale) et le TEK (Centre anti-terroriste).

ITALIE

En Italie, cette thématique est de la compétence de « *la Scientifica* » (Police Scientifique) qui dépend de la Direction Centrale Anti-crime. Les réponses apportées par le SSI Italie sont issues de ses échanges avec la section de la Police Scientifique en charge de l'analyse vidéo, l'analyse audio, l'analyse télématique, les interceptions et géolocalisations téléphoniques.

Il est à noter qu'en Italie l'article 9 du décret législatif du 08 octobre 2021 a énoncé **« la suspension » de l'installation et de l'utilisation de systèmes de vidéosurveillance utilisant des logiciels de reconnaissance faciale et fonctionnant grâce à l'utilisation de données biométriques**. Cette suspension est valable dans les lieux publics ou ouverts au public et concernent les installations émanant des entités publiques et privées. Cette suspension doit demeurer jusqu'à l'entrée en vigueur d'un cadre réglementaire précis en la matière et, en tout état de cause, jusqu'au 31 décembre 2023 (pas d'actualité).

L'Italie a donc fait partie des premiers pays de l'Union européenne à introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données biométriques, prévoyant également une amende administrative spécifique pour les contrevenants allant de 50 000 euros à 150 000 euros.

La suspension ne s'applique pas aux systèmes de vidéosurveillance qui n'utilisent pas de logiciels de reconnaissance faciale et qui sont donc conformes à la législation en vigueur. Ne sont donc pas visés le traitement des données effectué par les autorités compétentes à des fins de prévention et de répression des infractions ou d'exécution de sanctions pénales. Il est néanmoins nécessaire d'obtenir l'avis préalable favorable du « *Garant de la protection des données personnelles* » (**le Garant de la protection des données personnelles ou Garant de la Vie Privée est une autorité administrative indépendante instituée par la loi sur la protection de la vie privée n°675/1996**).

L'une des premières illustrations du nouveau cadre réglementaire date du 10 février 2022 et concerne la société Clearview AI. Le Garant de la protection des données personnelles, par injonction à l'encontre de Clearview AI, a obligé la société à supprimer les données relatives aux personnes qui sont situées en Italie et lui a interdit toute collecte et traitement ultérieur via son système de reconnaissance faciale. Il a également infligé à la société une amende de 20 millions d'euros. Il a été reproché à la société Clearview d'avoir mis en œuvre une véritable surveillance biométrique des personnes se trouvant sur le territoire italien.

Dans le domaine judiciaire, l'Italie utilise le **système SARI** (système automatique de reconnaissance faciale).

Le logiciel SARI est accessible et alimenté par les quatre Forces de l'ordre étatiques :Police d'État, les Carabiniers, la Guarde des Finances, et la Police pénitentiaire.

La nouveauté de ce système est qu'il est basé sur **une analyse morphologique globale** et plus uniquement sur un système de superposition ou de comparaison de photos anthropométriques.

Le projet SARI date de l'année 2016 . Les bases de données sont alimentées par la base de données AFIS (équivalent TAJ + photo + empreintes + signes particuliers + poids taille etc) et crée une data base SARI puis des applications SARI spécifiques (divers possibilités d'interrogation). Il compte actuellement plus de 9 900 000 clichés.

Par exemple, les services vont insérer une photo dans le logiciel qui après une analyse morphologique globale va proposer une liste de personnes susceptibles de correspondre, donnant un score de comparaison. L'analyse est ensuite reprise et affinée par des opérateurs manuels.

Il existe deux possibilités d'utilisation du logiciel SARI (par ex avec un cliché issu d'un système de vidéosurveillance) :

– Premier cas : **un suspect a déjà été identifié** par les enquêteurs et la demande de comparaison porte entre sa vraie photographie (document d'identité etc) et un cliché de vidéosurveillance. La comparaison des deux clichés sera complétée par une analyse morphologique globale. **Un procès verbal du résultat de cette analyse sera rédigé et pourra être utilisé devant un tribunal.**

– Second cas : **aucun suspect n'a été identifié par l'enquête.** La photo extraite de la vidéosurveillance va être insérée dans la base SARI qui va produire une liste d'individus pouvant correspondre qui sera ensuite traitée manuellement par un opérateur. **Le résultat de cette analyse ne pourra pas être utilisé en procédure mais constitue une aide à l'enquête.**

Enfin les Forces de l'ordre italiennes ont a leur disposition et utilisent ponctuellement le **logiciel « Briefcame »** (logiciel israélien) **qui permet de condenser en quelques minutes des heures de vidéosurveillance sur les seuls instants où il y a des mouvements**. Ce logiciel permet des interrogations multiples (homme, femme, véhicule, couleur, etc).

IRLANDE

Les autorités policières ont répondu par un état « néant » à toutes les questions. La police irlandaise intervient dans un cadre légal plus proche du contexte français. Force de taille par ailleurs modeste, aux moyens relativement limités et assez conservatrice dans l'exercice de ses missions, elle n'a pas du tout recours à ce jour aux logiciels d'analyse vidéo.

PAYS BAS

Les autorités néerlandaises n'ont pas encore répondu à la sollicitation du SSI. Leur retour vous parviendra à réception.

PAYS BALTES

En Estonie, le service de police et de garde-frontière n'utilise pas le logiciel Briefcam et n'a pas l'intention de commencer à l'utiliser.

En revanche, l'ASI a pu contacter la police municipale de Riga, en Lettonie, qui porte un intérêt à ce logiciel Briefcam. Voici les éléments de réponse :

1. *Quel logiciel utilisez-vous et quelles sont ses fonctions* ? (sélection de passages contenant des éléments d'intérêt, analyse comportementale, reconnaissance faciale, etc.)

La police municipale de Riga a l'intention d'utiliser Briefcam pour le contrôle du trafic, la reconnaissance faciale, l'analyse comportementale, la poursuite de criminels recherchés et pour simplifier les opérations de notre centre de vidéosurveillance. Le processus d'achat de Briefcam étant en cours, elle n'a pas encore commencé à utiliser le système, mais prévoit de le faire au début de l'année 2024.
Commentaire du SSI : la ville de Riga dispose d'un réseau de caméras très important, notamment sur les parties touristiques du centre-ville, dans les couloirs piétons souterrains, aux abords des bars et restaurants, etc. Le centre de supervision est armé 7j/7 et H24 par des policiers municipaux qui sollicitent des patrouilles au sol dès lors qu'un comportement suspect ou inapproprié est observé par une caméra, ou dès lors qu'un passant est potentiellement en difficulté.

2. *Quel cadre juridique définit cette utilisation* ?

La directive européenne sur la police et la loi locale sur la protection des données autorisent l'utilisation de la vidéosurveillance et de l'analytique à des fins de sécurité publique et de protection.

3. *Quelles sont les entités équipées* ?

Chacune des caméras – CCTV, véhicules de patrouille, drones et, dans un avenir proche, caméras corporelles – sera reliée et son flux vidéo transmis à la la plateforme Milestone. Par conséquent, l'analyse Briefcam sera intégrée à Milestone et fonctionnera à la fois avec des flux vidéo en ligne et des archives vidéo.

4. *Quels sont les contrôles appliqués à ce logiciel (est-il soumis à une validation préalable ? Dans quelles conditions ? Des personnes extérieures au cadre institutionnel ont-elles accès à leurs caractéristiques, notamment des personnes issues de la "société civile"* ?

Il s'agit d'un système restreint ; en raison de son caractère stratégique et de la nécessité de protéger les données à caractère personnel, l'accès est limité au personnel disposant d'une autorisation spéciale. Bien que le système soit principalement accessible au personnel chargé de l'application de la loi, un accès spécifique est accordé aux inspecteurs de la police criminelle ainsi qu'à d'autres membres de la société civile.

POLOGNE

Le bureau de la coopération internationale de police polonais, après avoir consulté les différentes unités, confirme que la police polonaise n'a pas accès aux outils logiciels d'analyse vidéo.

PORTUGAL

Le logiciel utilisé et ses fonctions (sélection des passages contenant des éléments d'intérêt tels que le dérushage, l'analyse comportementale, la reconnaissance faciale, etc.)

Sans objet

Le cadre juridique de son utilisation (judiciaire, administratif, etc.)

Le cadre juridique doit être envisagé sous deux angles :

1. Le régime de la loi sur la sécurité privée, cf. loi 34/2013 du 16 mai ;

2. Le régime qui réglemente l'utilisation et l'accès des forces et services de sécurité et de l'Autorité nationale d'urgence et de protection civile aux systèmes de vidéosurveillance pour la capture, l'enregistrement et le traitement d'images et de sons, est précise par la loi sur la sécurité Intérieure (loi 95/2001).

I - La loi sur la sécurité privée (loi 34/2013)

Cette loi établit également les mesures de sécurité à adopter par les organisations publiques ou privées en vue de protéger les personnes et les biens et d'empêcher la commission de délits, y compris l'utilisation de systèmes de vidéosurveillance.

Article 31 de la loi
Systèmes de vidéosurveillance
1 - Les entités titulaires d'un permis ou d'une licence pour l'exercice des services prévus à l'article 3, paragraphe 1, points a), c) et d), peuvent utiliser des systèmes de surveillance par caméra vidéo pour capter et enregistrer des images afin de protéger les personnes et les biens, à condition que les droits et les intérêts protégés par la Constitution soient préservés, et que leur enregistrement auprès de la direction nationale du PSP soit obligatoire, dans les conditions définies par décret du membre du gouvernement responsable du domaine de l'administration interne.
2 - Les enregistrements d'images obtenus par les systèmes de vidéosurveillance sont conservés dans un registre crypté pendant une période de 30 jours, à partir du moment où ils ont été capturés, après quoi ils sont détruits dans un délai maximum de 48 heures.
3 - Toute personne ayant accès aux enregistrements effectués en vertu de la présente loi, en raison de ses fonctions, est tenue de les garder confidentiels, sous peine de poursuites pénales.
4 - La cession ou la copie des enregistrements obtenus conformément à la présente loi est interdite et ne peut être utilisée qu'aux termes de la législation de procédure pénale.
5 - Dans les lieux surveillés par des caméras vidéo, il est obligatoire d'afficher, à un endroit bien visible, des informations sur les sujets suivants :
a) (Abrogé.)
b) La mention "Pour votre protection, ce lieu fait l'objet d'une vidéosurveillance" ;
c) L'entité de sécurité privée autorisée à exploiter le système, en mentionnant son nom et son permis ou sa licence ;
d) Le responsable du traitement des données collectées, auprès duquel les droits d'accès et de rectification

peuvent être exercés.
6 - Les mentions visées à l'alinéa précédent sont accompagnées des symboles appropriés, dans les conditions définies par arrêté du membre du Gouvernement compétent en matière d'administration interne.
7 - Les systèmes de vidéosurveillance doivent présenter les caractéristiques suivantes :
a) Possibilité pour les forces et services de sécurité d'accéder directement aux images en temps réel, à des fins de prévention ou d'enquête criminelle, en établissant un rapport motivé de l'événement ;
b) Système d'alarme permettant d'alerter les forces et services de sécurité territorialement compétents en cas de trouble, de risque ou de menace imminente pour la sécurité des personnes et des biens justifiant leur intervention ;
c) un registre des accès, comprenant l'identification des personnes qui y accèdent et la garantie de l'inviolabilité des données relatives à la date et à l'heure de leur collecte.
8 - Aux fins de l'alinéa précédent, les exigences techniques des systèmes de vidéosurveillance sont fixées par un arrêté du membre du gouvernement compétent en matière d'administration interne.
9 - L'enregistrement sonore par les systèmes visés au présent article est interdit, sauf autorisation préalable de la Commission nationale de protection des données, dans les conditions légales applicables.
10 - Les systèmes de vidéosurveillance, qui ne peuvent être utilisés que dans le respect des principes d'adéquation et de proportionnalité, doivent respecter les autres règles légales relatives à la collecte et au traitement des données à caractère personnel, notamment en ce qui concerne le droit d'accès, d'information, d'opposition des personnes concernées et le régime de sanction.

Aux termes de la loi susmentionnée, certaines entités sont obligées de disposer de systèmes de vidéosurveillance, comme les établissements de crédit et les sociétés financières, les pharmacies, les stations-service, entre autres.

II - Le régime qui régit l'utilisation et l'accès des forces et services de sécurité et de l'Autorité nationale d'urgence et de protection civile aux systèmes de vidéosurveillance pour la capture, l'enregistrement et le traitement d'images et de sons, qui renvoie à la loi sur la sécurité intérieure, cf. loi 95/2001, du 29 décembre, régit l'utilisation et l'accès des forces et services de sécurité et de l'Autorité nationale d'urgence et de protection civile (ANEPC) aux systèmes de vidéosurveillance pour la capture, l'enregistrement et le traitement d'images et de sons.
Cette loi s'applique aux systèmes de vidéosurveillance installés ou utilisés dans des espaces publics ou dans des espaces privés accessibles au public, lorsqu'ils sont dûment autorisés aux fins prévues à l'article suivant.
Article 3
Finalités du système
1 - Les systèmes de vidéosurveillance ne peuvent être utilisés qu'aux fins prévues par la loi sur la sécurité intérieure, approuvée par la loi n° 53/2008, du 29 août, et notamment pour
a) La protection des bâtiments et infrastructures publics et de leurs accès ;
b) Protéger les infrastructures critiques, les points sensibles ou les installations d'intérêt pour la défense et la sécurité, ainsi que leur accès ;
c) Soutenir l'activité opérationnelle des forces et services de sécurité dans le cadre d'opérations de police complexes, à savoir des événements de grande ampleur ou d'autres opérations à haut risque ou à menace élevée ;
d) la protection de la sécurité des personnes, des animaux et des biens dans les lieux publics ou dans les lieux auxquels le public a accès, et la prévention de la commission d'actes qualifiés par la loi d'infractions pénales dans les lieux où il existe un risque raisonnable qu'ils se produisent ;
e) Prévention des actes terroristes ;
f) Réponse opérationnelle aux incidents de sécurité en cours ;
g) Contrôle du trafic et sécurité des personnes, des animaux et des marchandises sur les routes ;
h) Prévention et répression des infractions routières ;
i) Contrôle de la circulation des personnes aux frontières extérieures ;
j) Protection des forêts et détection des incendies ruraux ;
k) Appui aux opérations de recherche et de sauvetage à l'extérieur.
2 - Aux termes de cette loi, il est également permis d'installer des systèmes de vidéosurveillance dans les locaux de la police qui servent au public.
D'une manière générale, il s'agit du cadre juridique qui définit le champ d'application et l'objectif des systèmes de vidéosurveillance.
III - En ce qui concerne les dispositions procédurales, il est fait référence à la loi n° 109/2009 du 15 septembre - la loi sur la cybercriminalité.

Les entités qui les utilisent (forces de sécurité de l'État, des régions et des communes, autres autorités locales, etc.)

Dans le cas de la vidéosurveillance sur la voie publique, les systèmes sont entièrement exploités par la police de sécurité publique.

Les contrôles auxquels ce logiciel est soumis (est-il soumis à une validation préalable ? Dans quelles conditions

? Des personnes extérieures au cadre institutionnel ont-elles accès à ses fonctionnalités, notamment des personnes issues de la "société civile" ?)

Dans le cas de la vidéosurveillance sur la voie publique, les demandes d'installation et d'utilisation sont adressées à l'autorité de contrôle pour autorisation, et le processus est toujours soumis à un avis de la Commission nationale de protection des données, portant sur les mesures de sécurité/protection des données et les caractéristiques techniques de l'équipement.

Si des controverses ou des litiges sont nés ou naissent à propos de ce logiciel et de ses fonctions, dans la sphère publique ou dans le cadre de procédures judiciaires, et comment ils ont été ou sont traités par les autorités, quelles en sont les conséquences, etc.

Sans objet

SLOVÉNIE

Les Slovènes précisent que les forces de police du pays n'utilisent pas ce type de logiciels.

II – **Pays hors Europe**

CORÉE DU SUD

Les logiciels utilisés et leurs fonctionnalités (sélection de passages comportant des items intéressants de type "dérushage", analyse comportementale, reconnaissance faciale…) :

La police coréenne utilise les logiciels suivants :
Amped five (le plus utilisé) : Équipé de filtres d'amélioration vidéo et utilisé pour des analyses de haut niveau telles que la reconnaissance faciale, la lecture des numéros d'immatriculation des véhicules, les analyses de comportements suspects. Temps d'analyse raccourci car sans processus d'extraction d'images.
Amped Athenticate : Application d'environ 25 filtres, comprenant l'analyse d'images pour détecter si elles ont été manipulées et retouchées par des logiciels «(*photoshopées* »). Analyse rapide des formats d'image pour analyser et mettre en avant les fichiers suspects.
Forensic Studio : Révision automatique par fonction marche/arrêt, affichage rapide des résultats des analyses et réglage facile des paramètres. Analyse rapide et accessible aux non-experts.

Le cadre juridique de leur utilisation (judiciaire, administratif…) :

L'utilisation des logiciels est autorisée dans le cadre judiciaire et administratif. Elle est facultative. La collecte d'informations est autorisée à des fins sécuritaires et encadrée en dehors de cet aspect (Loi sur la protection des informations personnelles).

Les entités qui les utilisent (forces de sécurité étatiques, régionales, municipales, autres collectivités territoriales…) :

Les logiciels sont utilisés par la police nationale coréenne, le ministère public, le service national de renseignement et l'armée coréenne.

Les contrôles dont ces logiciels font l'objet (sont-il soumis à validation préalable ? Selon quelles modalités ? Des personnes hors cadre institutionnel ont-elles accès à leurs caractéristiques, notamment des personnes issues de la "société civile" ?)

Les logiciels sont tous commercialisés à l'achat ou par abonnement. Amped Five fonctionne avec un dongle. Et ces dongles sont détenus par des analystes d'image qui sont au nombre de 23 en Corée, qui doivent suivre une formation professionnelle spécifique.
Si des polémiques ou des contestations ont eu lieu ou sont en cours sur ces logiciels et leurs fonctionnalités, respectivement dans l'espace public ou lors de procès, et la façon dont elles ont été/sont gérées par les autorités, leurs conséquences…

Le logiciel Amped Five est largement utilisé dans de nombreux pays, notamment aux États-Unis, au Royaume-Uni et en Italie. Il n'y a eu aucune controverse ni contestation quant à son utilisation comme preuve lors du procès puisqu'elle produit presque les mêmes images. De plus, le logiciel a été accrédité par le programme coréen d'accréditation des laboratoires pour l'analyse des plaques d'immatriculation des véhicules.

ROYAUME-UNI

Le Royaume-Uni se distingue par un cadre légal, un niveau d'acceptation sociale et un usage policier et sécuritaire de logiciels d'analyse variés particulièrement souples, aisés et répandus, en développement exponentiel.

Les logiciels utilisés et leurs fonctionnalités (sélection de passages comportant des items intéressants de type "dérushage", analyse comportementale, reconnaissance faciale…) :

Les 46 polices britanniques utilisent de nombreux logiciels dans des domaines très divers : surveillance de zone / agrégation de capteurs / détection d'anomalies par voie d'intelligence artificielle (en particulier le logiciel « Lattice », utilisé par la Border Force pour la surveillance des approches maritimes et la détection des « small boats »), vidéosurveillance et verbalisation routière directe (là aussi partiellement automatisée), transmission de dénonciations d'infractions routières constatée par voie de terminaux civils et pouvant donner lieu à verbalisation après visionnage par un opérateur police (https://nextbase.co.uk/national-dash-cam-safety-portal/), analyse comportementale à visée antiterroriste, lutte contre les vols à l'étalage, etc.

Le cadre juridique de leur utilisation (judiciaire, administratif…) :

Le cadre juridique est particulièrement souple, et explique un foisonnement d'outils de captation et d'analyse vidéo, publics et privés, avec un niveau de densité et une simplicité de mise en place sans équivalent dans d'autres pays occidentaux.

Les entités qui les utilisent (forces de sécurité étatiques, régionales, municipales, autres collectivités territoriales…) :

Acteurs publics, policiers ou non (autorités communales, gestion des déchets, des flux de transport, etc.), privés, (chaînes de supermarchés, entreprises de tout type, particuliers). La police a un accès assez libre et souple à de nombreuses sources, pour du renseignement mais aussi ses enquêtes ou de la verbalisation.

Les contrôles dont ces logiciels font l'objet (sont-ils soumis à validation préalable ? Selon quelles modalités ? Des personnes hors cadre institutionnel ont-elles accès à leurs caractéristiques, notamment des personnes issues de la "société civile" ?

Il n'y a pas de validation préalable, l'accès est libre et un contrôle peut avoir lieu *a posteriori* ou sur demande/dénonciation par une autorité administrative indépendante.

Si des polémiques ou des contestations ont eu lieu ou sont en cours sur ces logiciels et leurs fonctionnalités, respectivement dans l'espace public ou lors de procès, et la façon dont elles ont été/sont gérées par les autorités, leurs conséquences…

Il existe des organisations et mouvements hostiles aux logiciels d'IA appliqués à la vidéoprotection (par exemple https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/), y-compris au sein du parlement britannique. Ils restent minoritaires au sein d'un pays très fortement équipé et novateur en la matière. Le degré d'acceptation sociale de ces technologies demeure très élevé et permet aux polices britanniques d'expérimenter et d'utiliser assez librement de nouvelles solutions.

Commentaires

Le Royaume-Uni est en pointe sur l'utilisation de logiciels d'analyse et les applications policières de l'intelligence artificielle, rendues possibles par une culture interne favorisant l'innovation et un cadre légal particulièrement permissif.

Les points évoqués supra ont fait l'objet de plusieurs notes d'information plus détaillées de la part du SSI, que la DCIS tient à disposition de l'IGA.

CANADA

Note préliminaire : étant donné le caractère sensible de la thématique, à la suite d'une polémique d'ampleur (affaire Clearview IA) le caractère d'une partie des informations recueillies par le SSI doit être considéré comme **provisoire** (pas de réponse consolidée des partenaires). Une mention est faite lorsque nécessaire.

Actuellement au Canada, les services de police n'utilisent que partiellement des logiciels d'analyse vidéo ou de reconnaissance faciale, mais souhaiteraient pouvoir élargir le cadre d'emploi. La gendarmerie royale du Canada (GRC, seule force fédérale) a récemment dû se mettre en conformité selon les recommandations formulées par le Commissariat à la protection de la vie privée (~CNIL), à la suite d'une enquête menée à son encontre en 2020 pour l'emploi du logiciel Clearview AI, qui avait fait l'objet d'un piratage de données.

Dans ce contexte, une réflexion générale est en cours sur l'amélioration du cadre juridique fédéral concernant l'utilisation, l'interdiction, la surveillance et la confidentialité des outils d'analyse vidéo et de reconnaissance faciale par les services de police fédéraux et provinciaux.

Contexte canadien :

- **Les services de niveau fédéral, dont la Gendarmerie royale du Canada (GRC), sont chargés de l'application des lois fédérales sur l'intégralité du territoire canadien.**
- Pour le reste, au total, près de 80 000 policiers sont répartis dans 180 forces très différentes les unes des autres en doctrine, moyens et politique d'équipement. Ils dépendent également de règlements et textes provinciaux (souvent adaptés du niveau fédéral), y compris pour ce qui concerne la conservation des données, les libertés publiques etc.
- **Les services de niveau provincial** (seuls l'Ontario, le Québec et Terre-Neuve disposent d'une force spécifique provinciale) **sont chargés de l'application du code criminel et des lois provinciales, dans des zones non couvertes par une force municipale.** Les autres provinces et territoires **agissent par contrat**, en déléguant l'action de sécurité à la GRC, qui agit alors comme force territoriale.
- **Les services de niveau municipal sont chargés de l'application du code criminel, en l'absence de force provinciale spécifique ou de contrat avec la GRC.** Les services de police de Montréal, Toronto, Vancouver ou Edmonton en sont quelques exemples.

1. Une utilisation partielle des logiciels d'analyse vidéo et de reconnaissance faciale

Les différents services de police canadiens n'utilisent que partiellement les logiciels d'analyse vidéo et de reconnaissance faciale.

Cependant, on peut noter quelques exemples, tel que la police de Calgary depuis 2014, qui a été **la première au Canada à annoncer l'utilisation de la reconnaissance faciale pour ses besoins d'enquête** (le SSI reste en attente d'une réponse consolidée de leur part).

La **police d'Edmonton en Alberta,** a annoncé avoir recours à la technologie de reconnaissance faciale depuis le **début de l'année 2022,** en premier lieu pour faciliter l'identification des personnes impliquées dans des enquêtes criminelles ou placées en garde à vue, qui pourraient fournir de fausses informations sur leur identité. Elle se sert du logiciel **NeoFace Reveal**, créé par l'entreprise texane *NEC Corporation of America*. La police d'Edmonton a d'ailleurs ajouté qu'elle partageait une base de données avec la police de Calgary.

Grâce à son partenariat conclu en 2021 avec la société Idemia (société française), la **Sûreté du Québec** peut exploiter ce type de technologie dans le cadre d'enquêtes criminelles, afin de comparer des images vidéo à celles de sa banque de données, comptant des dizaines de milliers de photos signalétiques.

2. Un cadre juridique complété par des lois issues des gouvernements provinciaux

Les commissaires à la protection de la vie privée à l'échelle fédérale, provinciale et territoriale estiment que le contexte législatif actuel entourant l'utilisation de la technologie de reconnaissance faciale par les services de police est insuffisant. Pour eux, *« En l'absence d'un cadre juridique complet, une incertitude importante demeure quant aux situations dans lesquelles l'utilisation de la RF par les services de police est légale ».*

De multiples sources de fondement juridique

Il n'existe pas de cadre juridique précis pour l'utilisation de la reconnaissance faciale au Canada. Le cadre juridique est plutôt constitué d'une mosaïque faisant intervenir des lois et la *common law*. Il s'agit notamment des lois fédérales et provinciales sur la protection des renseignements personnels, des lois régissant les pouvoirs et les activités des services de police et de la jurisprudence relative à la Charte canadienne des droits et libertés. **La loi sur la protection des renseignements personnels**[2] définit néanmoins les conditions dans lesquelles les organismes publics peuvent recueillir, utiliser, communiquer et conserver les renseignements personnels. Dans certaines provinces, le cadre juridique peut être toutefois plus spécifique.

À ce jour, **le Québec** est la **seule province** dotée d'une loi qui **traite précisément des données biométriques**, lesquelles englobent celles que vise la **technologie de reconnaissance faciale**. La loi définissant le cadre juridique des technologies de l'information du Québec exige que la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement déclarée à la Commission d'accès à l'information. Cette autorité peut par la suite interdire la mise en service d'une telle base de données, ordonner que des changements y soient apportés, ou en ordonner la destruction. De plus, tout autre renseignement concernant une personne qui pourrait être découverte à partir des caractéristiques ou mesures biométriques ne peut servir à fonder une décision à son égard.

2 https://laws-lois.justice.gc.ca/FRA/LOIS/P-21/index.html

Autorisation judiciaire et pouvoirs conférés par la loi

Les services de police peuvent demander et obtenir l'autorisation judiciaire de recueillir et d'utiliser des empreintes faciales dans les situations qui justifient une telle intervention. L'article 487-01 du Code criminel prévoit la délivrance de mandats qui autorisent une intrusion dans la vie privée d'une personne « lorsqu'un juge est convaincu : qu'il existe des motifs raisonnables de croire qu'une infraction a été ou sera commise et que des renseignements relatifs à l'infraction seront obtenus grâce à une telle utilisation ou à l'accomplissement d'un tel acte; que la délivrance du mandat servirait au mieux l'administration de la justice d'agir; et dans les situations pour lesquelles il n'existe aucun fondement juridique permettant d'intervenir en ce sens ».

Les services de police peuvent également invoquer des lois précises pour justifier le bien-fondé de leurs interventions. Par exemple, à des fins d'identification, la loi sur l'identification des criminels permet aux services de police de prélever des empreintes digitales ou de photographier des personnes accusées ou déclarées coupables de certains crimes. Elle autorise aussi la publication de ces éléments d'identification afin de fournir des renseignements aux policiers et aux autres personnes chargées de l'application ou de l'exécution de la loi. La Loi sur l'identification des criminels n'autorise cependant pas la collecte arbitraire de photographies d'autres personnes au sein de la population en général.

3. Les suites de l'affaire Clearview IA : une nécessaire mise en conformité de la GRC

Dans le contexte de la polémique concernant l'utilisation d'un logiciel de reconnaissance faciale, dénommé **Clearview AI,** par la Gendarmerie royale du Canada (GRC) et 34 autres services de police, le Commissariat à la protection de la vie privée du Canada **avait lancé une enquête en 2020**, en vertu de la loi canadienne sur la protection des renseignements. En effet, une liste volée de plus de 2 200 clients de l'entreprise avait conduit plusieurs services de police à communiquer sur l'usage de ce logiciel. La GRC (notamment pour les enquêtes de pédopornographie), la Police provinciale de l'Ontario et la Police de Toronto ont confirmé avoir eu recours à ce logiciel pour des enquêtes spécifiques personnels, ainsi **une enquête à leur encontre avait également été dirigée**. La GRC aurait notamment effectué plus de 450 recherches avec ce logiciel.

Par la suite, un **rapport spécial du Parlement**[3] et **un document d'orientation conjoint** ont été publiés par le Commissariat à la protection de la vie privée du Canada, le 10 juin 2021. Il transmet les conclusions de l'enquête sur l'utilisation de la GRC de la technologie de Clearview en affirmant qu'elle a bien **contrevenu à la loi sur la protection des renseignements personnels**, en recueillant des renseignements personnels auprès de Clearview AI. En l'espèce, une institution fédérale ne peut recueillir de renseignements personnels auprès d'un tiers si celui-ci les a recueillis illégalement. La GRC a reconnu publiquement qu'elle l'avait seulement utilisée de manière limitée, principalement pour identifier, retrouver et sauver des enfants exploités sexuellement sur Internet. Toutefois, selon l'enquête, la GRC n'aurait pas été en mesure de rendre compte de manière satisfaisante de la grande majorité des recherches qu'elle a effectuées.

Concernant le **document d'orientation**[4] **(mai 2022)**, il est à l'intention des services de police quant à l'usage de la reconnaissance faciale. Élaboré conjointement avec les homologues provinciaux et territoriaux au Canada, ce document d'orientation préliminaire a pour objectif de **préciser les obligations des services de police en matière de protection de la vie privée** relativement à l'utilisation de la technologie de reconnaissance faciale, afin d'assurer que l'utilisation de celle-ci soit conforme aux lois actuelles et limite les risques d'atteintes à la vie privée.

Ainsi, deux ans plus tard, le Commissariat à la protection de la vie privée a constaté dans son **rapport annuel au Parlement** 2022-2023[5], que la **GRC a bien mis en œuvre ses recommandations** et qu'elle a pris des mesures pour créer une culture qui favorise la conformité au moment de commencer à utiliser de nouvelles technologies donnant lieu à la collecte de renseignements personnels.

Il est à noter que la GRC **n'a plus recours à la technologie de Clearview AI** puisque l'entreprise a cessé d'offrir ses services au Canada en juillet 2020, suite à l'enquête du Commissariat à la protection de la vie privée. (attente d'une réponse consolidée de leur part).

D'autres solutions sont à l'étude, sous le contrôle d'un bureau spécifique au sein de la GRC (Programme national d'intégration des technologies-PNIT) qui offre des analyses sur la légalité des outils permis par les nouvelles technologies (dont l'IA) pour les besoins opérationnels des unités de la GRC.

Commentaire :

Le gouvernement envisage actuellement de moderniser le régime de protection de la vie privée et des données du Canada dans la perspective que les services de police intègrent la technologie de reconnaissance faciale dans leurs activités (et d'autres, caméra-piétons, IA, ADN généalogique etc). Toutefois, il reste encore à élaborer un cadre réglementaire fédéral plus effectif encore concernant les utilisations, les interdictions, la surveillance et la confidentialité de ces outils émergents.

3 https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/

4 https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/surveillance/police-et-securite-publique/gd_rf_202205/

5 https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202223/ar_202223/

ÉTATS-UNIS

1) Tour d'horizon de l'utilisation des logiciels d'analyse vidéo par les services de police

Aux États-Unis, les logiciels d'analyse vidéo ne sont pas utilisés par la majorité des 18 000 services de police que compte le pays, cependant la grande majorité des agences ayant adopté cette technologie utilise l'outil développé par la société *Briefcam*. **Cette technologie baptisée VSA (*Video Surveillance Algorithm*) outre-Atlantique**, adaptée au traitement d'importants flux vidéo, est principalement déployée dans les comtés ou villes à forte densité de population, ou le long de la frontière sud des États-Unis afin de discriminer les passages de clandestins sur des milliers d'heures d'enregistrement vidéo, dont le traitement humain serait particulièrement chronophage. Le logiciel analyse les productions des dizaines de caméras raccordées au système et sélectionne les séquences ou apparaissent les items choisis par l'opérateur, tels qu'une tenue vestimentaire, un véhicule spécifique ou, pour les dernières versions, un comportement prédéfini.

Les techniques de surveillance des services de police n'étant pas toujours tenues secrètes, un site spécialisé[6] répertorie sur l'ensemble du territoire américain (5 500 juridictions administratives), les solutions et outils technologiques utilisés par les services répressifs. Cela va de l'emploi des caméras-piétons jusqu'à la VSA, en passant par les lecteurs automatisés de plaques d'immatriculation, ou la reconnaissance faciale.

Ainsi, la VSA ne serait utilisée que par une cinquantaine de services de police, l'option de reconnaissance faciale n'étant, dans la quasi-totalité des cas, pas autorisée par les municipalités dans le cadre de l'analyse de flux vidéo. Pour autant, les agences américaines ne se privent pas d'utiliser ces outils spécifiques pour faciliter la résolution d'enquêtes criminelles. Cependant, qu'ils s'agissent d'outils développés par des sociétés privées ou inclus dans des bases de données photographiques gérées par des services locaux ou fédéraux, le recours à la reconnaissance faciale est très encadré et les opérateurs doivent recevoir une formation spécifique afin d'être habilités à l'utiliser. Les comparaisons se font à partir de bases de données photographiques locales, ou spécifiques à une agence, les États-Unis n'étant pas dotés de fichiers nationaux destinés à cet usage. Par exemple, le comté de Los Angeles dispose du LACRIS[7] (*Los Angeles County Regional Identification System*) qui regroupe les photos et données biométriques des criminels arrêtés dans le comté. LACRIS possède des fonctionnalités telles que la comparaison d'empreintes digitales, d'iris ou la reconnaissance faciale, et propose en outre une application mobile qui effectue des comparaisons d'empreintes et d'iris en 30 secondes. Toutes les fonctionnalités du système, y compris l'utilisation de la reconnaissance faciale, font l'objet d'une réglementation[8] spécifique pour ses utilisateurs.

L'État du Maryland, a développé depuis 2011 un outil de reconnaissance faciale intégré dans une base de données baptisée MIRS (*Maryland Image Repository System*) qui comprend plus de dix millions de photographies des détenteurs de permis de conduire et des criminels arrêtés dans l'État. De plus le système MIRS balaye également la base de données du FBI qui compte plus de 25 millions de clichés.

S'agissant de la VSA, utilisant ou pas l'option de reconnaissance faciale, il n'existe pas de réglementation fédérale précise relative à son emploi. Toutefois, plusieurs décrets présidentiels, destinés à promouvoir et encadrer l'utilisation de l'intelligence artificielle au sein des agences gouvernementales recommandent de n'utiliser que des outils dignes de confiance, qui garantissent également le respect des droits civiques de la population américaine. La VSA utilisant très largement l'IA, son utilisation se doit de respecter les critères définis par la Maison-Blanche.

À moindre niveau, ce sont les États et les municipalités qui votent les budgets pour leurs services de police respectifs, qui décident ou pas de son utilisation, en accord avec les citoyens et les associations de défense de leurs droits. La validation préalable de l'utilisation de ce type de logiciels s'effectue donc en amont, lors des débats des assemblées locales, où les conditions d'utilisation et les financements sont soumis aux votes des élus locaux. Des décisions d'interdiction *a posteriori* définitives ou temporaires sous forme de moratoire, peuvent néanmoins être prononcées, à l'instar de Baltimore dans le Maryland, où le conseil municipal a interdit en août 2021 l'utilisation de la technologie de reconnaissance faciale par les organismes publics et privés de la ville.

2) Les autres entités qui utilisent des logiciels d'analyse vidéo

Sur son site commercial, la société *Briefcam*, fondée par des chercheurs israéliens en 2007 puis rachetée par Canon en 2018, promeut l'utilisation de son logiciel d'analyse par nombre de services répressifs américains, mais aussi par d'autres entités telles que des hôpitaux ou des universités.

L'hôpital général du Massachussetts[9] qui est composé d'un établissement principal situé sur un terrain de sept hectares et de nombreuses annexes dans la métropole de Boston, emploie 30 000 personnes et reçoit

6 https://atlasofsurveillance.org/

7 https://lacris.org/

8 https://lacris.org/LACRIS%20Facial%20Recognition%20Policy%20v2.0%2006.23.pdf

9 *Massachusetts General Hospital (MGH)*

chaque jour 60 000 patients et visiteurs. Le service de sécurité de l'établissement, qui s'appuie sur environ quelque 13 000 caméras sur l'ensemble de ses sites, s'est doté de la solution *Briefcam* afin d'analyser en quelques minutes des heures d'enregistrement vidéo, en cas d'incident ou d'intrusion d'individus ou de véhicules non autorisés dans son périmètre.

Les établissements universitaires américains dont les campus s'étalent généralement sur plusieurs hectares et abritent des milliers d'élèves, prennent leur sécurité très au sérieux, d'autant que plusieurs ont été le théâtre de tueries de masse au cours des dernières années. La vidéo surveillance y est largement utilisée, ces établissements se dotant de plus en plus de technologies VCA leur permettant de vérifier en temps réel les véhicules autorisés à pénétrer sur le campus, de retrouver des étudiants portés disparus ou de détecter des comportements suspects.

3) Exemple de services partenaires utilisant la VSA

Le SSI a récemment pris contact avec le *United States Park Police (USPP),* qui utilise la solution *Briefcam* sur le *National Mall*[10] de Washington DC. Dans l'attente d'une démonstration pratique, les informations suivantes concernant son utilisation lui ont été transmises :

- L'USPP n'a pas besoin d'autorisation préalable ou de validation particulière pour utiliser la technologie d'analyse vidéo. Le Chef de ce service ayant indiqué que l'utilisation de cet outil était nécessaire au bon accomplissement de sa mission, la requête a été validée par son autorité de tutelle. À ce jour l'utilisation de la VSA par l'USPP, très médiatisée en sources ouvertes, n'a pas suscité de polémiques ou de contestations au sein de la population de Washington DC.

- S'agissant de fonctionnalités particulières telles que la reconnaissance faciale, elle ne peut être utilisée qu'avec l'accord de la justice en cas d'infraction commise sur le ressort de l'USPP, et après délivrance d'un mandat spécifique.

- Enfin, l'USPP a précisé que cette solution d'analyse video leur avait été offerte par la société *Briefcam.*

La police du comté de Fairfax en Virginie (FCPD) a indiqué être en train de mettre en place un *Real Crime Center* qui va centraliser, sur des murs d'écrans, l'ensemble des flux vidéo de toutes les caméras installées sur son ressort.

Ce centre, que le SSI a été invité à visiter dès son inauguration prochaine, va non seulement permettre de prendre la main en temps réel sur les caméras de surveillances, mais aussi d'utiliser *a posteriori* des logiciels d'analyse vidéo, couplés avec d'autres technologies telles que les lecteurs automatiques de plaques d'immatriculation[11] pour identifier et localiser des auteurs de crimes et délits. Les contraintes administratives pour la mise en place de ce système sont limitées à une expression de besoin du chef du FCPD pour obtenir les fonds du comté, puis à la rédaction d'une *Standard Operating Procedure* (SOP), forme de doctrine d'emploi, pour encadrer ses règles d'utilisation.

Il a été confirmé au SSI que la seule contrainte légale serait l'interdiction « pour le moment » de la reconnaissance faciale.

Enfin le FBI, qui a très largement utilisé cette technologie lors de l'attentat du marathon de Boston afin de traiter des centaines d'heures d'enregistrements vidéo fournies par le public, devrait répondre à la sollicitation du SSI de visiter leurs infrastructures dédiées. **Le cas échéant, un additif à la présente note sera alors rédigé.**

Commentaires :

À l'instar de nombre de technologies qui concourent à assurer la sécurité de la population, les logiciels d'analyse vidéo sont fréquemment utilisés par les services de police américains lorsqu'ils s'avèrent nécessaires au bon accomplissement de leur mission. De nombreuses polices municipales mettent en place des Real Crime Center, comme celui de la police de Washington DC, qui devrait être inauguré en début d'année.
Ce nouveau centre aura la particularité de fusionner avec ceux des villes et comtés limitrophes pour étendre la surveillance vidéo au-delà des frontières de la capitale fédérale et fera un large usage de la technologie VSA afin de traiter les flux vidéo de centaines de caméras de surveillance.

La seule restriction actuelle concerne l'utilisation de la reconnaissance faciale, qui pour l'instant, reste soumise à un encadrement législatif spécifique.

10 Parc ouvert au public s'étalant du Lincoln Mémorial au Capitol bordé par de nombreux musées, monuments et mémoriaux.
11 Cf Note DCIS 214-2023-Les services de police américains continuent de se doter de systèmes de type LAPI

Partie II : Point sur les dernières orientations de l'UE sur le sujet (emploi d'outils d'analyse vidéo de masse, y compris en matière d'utilisation de la reconnaissance faciale) et sur l'avancée du projet TELEFI (Towards the European Level Exchange of Facial Images)

Réponse fournie par le Commissaire général de police, Conseiller Affaires intérieures à Bruxelles :

Pour la partie relative à la reconnaissance faciale, vu de la représentation permanente française auprès de l'Union européenne, il n'y a pas en l'état de projets particuliers. Le sujet est surtout évoqué dans le cadre des négociations sur le **règlement RIA** (projet de règlement sur l'intelligence artificielle), à travers « l'identification biométrique » -RBI- en temps réel et *a posteriori*.

Il existe une forte opposition du Parlement européen pour la reconnaissance faciale, mais le compromis va permettre – en principe, car la représentation permanente n'a toujours pas accès au texte, et les considérants sont en discussion – de limiter les contraintes aux seules identifications à distance (*remote*). Cela exclut les vérifications d'identité ; il reste toutefois à s'assurer que la vérification d'identité, avec l'individu sur place et une identification à distance via une base de donnée, ne fasse pas partie du périmètre de ces restrictions.

Les RBI en temps réel seront strictement limitées (liste d'infractions, autorisation par une autorité indépendante, situations de risque imminent, etc.) et seront *a posteriori* soumises à des limitations, notamment pour identifier précisément une personne – hors recherche d'empreintes pour identifier un suspect inconnu - avec notamment une autorisation requise (y compris par une autorité administrative pouvant ne pas être indépendante, et dans les 48 h). Beaucoup de questions se posent encore sur la mise en œuvre.

Enfin, pour le projet **TELEFI**[12], la représentation permanente n'a pas à ce jour d'autre information que celle indiquée au lien suivant : https://www.telefi-project.eu/telefi-project/about-telefi-project. Les résultats sont précisés au lien suivant : https://www.telefi-project.eu/telefi-project/results.

Remarque :

Le Conseiller aux Affaires Intérieures souhaiterait en retour être destinataire d'une communication officielle ou des éléments de langage de la France (et si possible du MIOM), par rapport à des accusations d'usage par la police française de Briefcam, hors encadrement légal[13].

À défaut, pourriez-vous nous faire parvenir une communication officielle éventuelle sur le sujet, si une telle communication était élaborée (cadre **EDL**), pour l'aider le cas échéant à répondre aux interrogations possibles des partenaires à Bruxelles ?

12 Le projet TELEFI (*Towards the European Level Exchange of Facial Images*) mène une étude sur la manière dont la reconnaissance faciale est actuellement utilisée dans les États membres de l'UE pour les enquêtes pénales relatives à des infractions graves. En outre,il sera étudié la possibilité de s'appuyer sur le cadre du traité de Prüm pour mettre en œuvre l'échange d'images faciales, comme c'est le cas actuellement pour les profils ADN, les empreintes digitales et les données d'immatriculation des véhicules.

13 Interrogations de la Commission à ce sujet : « En 2015, les forces de l'ordre ont acquis, en secret, un logiciel d'analyse d'images de vidéosurveillance de la société israélienne Briefcam. Depuis huit ans, le ministère de l'Intérieur dissimule le recours à cet outil qui permet l'emploi de la reconnaissance faciale » - https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale.

Source : DCIS sur la demande de la mission, janvier 2024

Annexe n° 5 : Les « solutions » du logiciel *BriefCam* et leurs fonctionnalités

BriefCam

TRANSFORMER LA VIDÉOSURVEILLANCE EN INTELLIGENCE ACTIVE

BriefCam est proposé dans un certain nombre de variantes comme détaillé dans le tableau ci-dessous :

Variante	BriefCam Investigator	BriefCam Investigator4Teams	BriefCam Rapid Review	BriefCam Insights	BriefCam Protect
Sources vidéo	Fichiers	Fichiers	VMS	VMS	Fichiers et VMS
Solutions incluses	REVIEW	REVIEW	REVIEW	REVIEW, RESEARCH, RESPOND	REVIEW, RESEARCH, RESPOND
Nombre d'utilisateurs	Utilisateur unique	Multi utilisateurs	Multi utilisateurs	Multi utilisateurs	Multi utilisateurs

Solutions logicielles BriefCam

La plate-forme BriefCam comprend les modules clés suivants :

La solution REVIEW - permet la génération de VIDEO SYNOPSIS® sur la base de vidéos provenant de fichiers hors-ligne et de plateformes VMS en ligne, avec une gestion complète des cas et des fonctionnalités puissantes telles que la recherche multi-caméras, la similarité d'apparence et la reconnaissance faciale.

La solution RESEARCH - facilite l'exploitation des renseignements dérivés de l'analyse vidéo quantitative pour une prise de décision informée et basée sur les données, y compris les analyses de tendances avancées et dimensionnelles d'indicateurs de performance (zone, trajectoire, durée et autres) ainsi que les fonctionnalités de tableau de bord et de planification.

La solution RESPOND - prend en charge la fourniture de réponses proactives aux événements critiques pour une sûreté et une sécurité accrue, avec des alertes personnalisables, des rapports d'alerte et des notifications par internet.

Page 5 de 208 © BriefCam | 11/2/20

Source : Manuel utilisateur BriefCam - septembre 2020 -

Annexe n° 6 : Les licences *BriefCam* dans la police nationale

SERVICE	Nombre de Licences	Remarques	Utilisations de Briefcam (hors reconnaissance faciale qu'aucun service n'utilise)	Licence incluant la reconnaissance faciale	Versions logiciel	Nombre d'utilisateurs	Implantation du logiciel
DCPJ/SDAT	1		1	Non	4.0	1	Levallois-Perret
DCPJ/ SIAT National	1		0	Oui	6.2		Nanterre
DZPJ NORD/Antenne SIAT	3	Utilisés pour DZPZ,DZSP et DZPAF	5 à 6 par an	Non	4.3	9	Lille Lens Amiens
DZPJ EST	1	Module incompatible avec les ordinateurs dédiés	0	Oui	5.3	3	Dijon
DZPJ SUD EST Antenne SIAT	1		ponctuellement	Oui	6.2	7	Lyon
DZPJ SUD	4	Nice,licence achetée DDSP et utilisée par PJ	Marseille: 0 Nice: 1 par an Ajaccio : 2 Bastia: 1 par semaine	Oui	5.4 5.6	4	Marseille Nice Ajaccio Bastia
DZPJ SUD OUEST Antenne SIAT	3		Bordeaux: 6 Bayonne : 0 Limoges : 4	Oui	5.3 5.4 5.4	8	Bordeaux Bayonne Limoges
DZPJ OUEST Antenne SIAT	4		19	Oui	5.3 5.4 Ignoré 5.4	11	Rennes Nantes Orléans Rouen
DRPJ VERSAILLES	4		Versailles: 2 par mois Meaux:1 par semaine Evry : 0 Cergy : rarement	Oui	6.4 6.2 6.2 6.4	9	Versailles Meaux Evry Cergy
DZSP NORD USI 59	1		13	Oui	6.0	2	Lille
DZSP SUD EST	0	Licence payée par DZSP mais logiciel utilisé par le SIAT	0				
DZSP SUD	1	Nice, utilisé par PJ	55	Oui	5.6 5.6	1	Nice Toulouse
DDSP Grande Couronne	2		20	Oui	6.0 6.2	10	Melun Cergy
DTPN 971	1		0	Oui	6.4	0	Pointe-à-Pitre
DTPN 972	1	Licence périmée au 03/12/2020	1	Non	5.4	0	Fort-de-France
IGPN	2		0	Non	5.7 5.7	0	Délégation Paris Délégation Marseille
SNPS	1		3	Oui	6.0	NC	Ecully
PP/DSPAP/UAT	1	Licence acquise sur fonds MILDECA en 2016, devenue obsolète en 2022 faute de financement pour le renouvellement	30	Non	NC	6	Paris

Source : DNPJ, retravaillée par la mission, et entretien avec la DSPAP de la préfecture de police

Annexe n° 7 : Les licences *BriefCam* dans la gendarmerie nationale

FORMATION ADMINISTRATIVE DE RATTACHEMENT	NOM DE L'UNITÉ	ADRESSE	NOMBRE DE LICENCES POSSÉDÉES...	...DONT CELLES INCLUANT LA RECONNAISSANCE FACIALE	ENCORE FONCTIONNELLE AU 17/11/2023 (DATE DU MESSAGE DE SUSPENSION) ?	FRÉQUENCE D'UTILISATION DE BRIEFCAM (SUR LES 2 DERNIERES ANNEES)	UTILISATION DE BRIEFCAM ACTÉE EN PROCÉDURE ?	VERSIONS	DATE D'ARRIVÉE DANS LE SERVICE	NOMBRE D'UTILISATEURS DANS L'UNITÉ	EXEMPLE D'AFFAIRES MARQUANTES OÙ BRIEFCAM A ÉTÉ DÉTERMINANT	OBSERVATIONS DIVERSES
SDPJ	OCLDI	6 Avenue de Stalingrad - 94110 ARCUEIL	1	x	OUI	une douzaine de dossiers	NON	5.3	Janvier 2019 (date d'installation de la version)	2 militaires	Néant	NÉANT
PJGN	SCRCGN	5 boulevard de l'Hautil 95000 Pontoise	1	x	OUI	4 utilisations	NON	6.3	Février 2018 (mise à jour juin 2023)	02 utilisateurs	Enlèvement séquestration sur fond de trafic international de stupéfiants	En 2023, 5 dossiers ont été renvoyés aux unités suite à la suspension de l'utilisation de l'outil. 1 à 2 utilisations de l'outil par an depuis 2018.
RGCOR	SR AJACCIO	Camp d'Aspretto AJACCIO	1		OUI	10 utilisations	NON	4.3	Février 2018	4 à 6 militaires sur l'ensemble des deux détachements de la SR (matériel partagé)	Néant	Néant
RGHF	SR AMIENS	107 rue d'elbeuf 80000 AMIENS	1		OUI	10 utilisations	NON	4.3	mai 2018	01 militaire	0	Problèmes d'intégration suite aux multiples formats de vidéos propriétaires. Impossibilité de les convertir.
RGPL	SR ANGERS	33, rue du nid de pie ANGERS 49000	1		NON	10 utilisations	NON	4.3	Février 2018	6	Homicide – Tentative Homicide - Disparition – Enlèvement – Recel	1ère version Briefcam, non munie de la reconnaissance faciale.
RGBFC	SR BESANCON	CASERNE CAPITAINE GIRARD 26 RUE DES JUSTICES 25031 BESANCON CEDEX	1		OUI	10 utilisations	NON	4.3	Février 2018	01 militaire (référent) formé initialement à la mise en place de la solution Briefcam Formation étendue par ce militaire à l'ensemble des personnels de l'unité	Exploitation vidéosurveillance cadre diverses affaires (homicides, attaques de DAB, etc)	
RGNA	SR BORDEAUX	Quartier Bételle 33270 BOULIAC	1		NON	0 sur les 2 dernières années	NON	4.3	Février 2018	1 militaire	Aucun	Produit non utilisé et non mis à jour
RGCVL	SR BOURGES	173 AVENUE DE SAINT-AMAND 18000 BOURGES	1		OUI	8 utilisations	NON	4.3	Février 2018	4 militaires	vols en BO – homicide – enlèvement séquestration	
RGNORM	SR CAEN	29 avenue du 43eme RA 14000 CAEN	1		OUI	5 utilisations	NON	4.3	Février 2018	1 militaire formé et utilisateur principal 3/4 militaires de l'unité initiés	Utilisation déterminante dans des dossiers d'homicide ou tentative	Néant
RGARA	SR Chambéry	28 rue de Sonnaz, 73000 Chambéry	1		OUI	20 utilisations	NON	4.3	Février 2018	15 militaires		Le logiciel Briefcam est utilisé pour exploitation des vidéos des dossiers de CrimOrg de la SR mais jamais acté en procédure. Il devait être utilisé par le SCRC pour le traitement de vidéos dans le cadre de l'homicide de la policière à La Rochette (73).
RGARA	SR CLERMONT-FERRAND	48 RUE DU TORPILLEUR SIROCCO	1		OUI	6 utilisations	NON	4.3	Février 2018	5 militaires	Stupéfiants	Découverte d'une cache en forêt - application a permis d'analyser les enregistrements H24 7/7 avec des durées d'exploitation beaucoup chronophages
RG BOURGOGNE FRANCHE-COMTE	SR DIJON	Quartier DEFLANDRE - 30 boulevard Maréchal Joffre - 21000 DIJON	1		NON	4 utilisations	NON	4.3	Mai 2018	4 militaires	Trafic de stupéfiants - Vols de BO (vidéo de la ville ou péages)	
COMGENDMQ	SR FORT-DE-FRANCE (972)	CASERNE REDOUTE BP 616 97261 FORT DE FRANCE CEDEX	1		OUI	10 utilisations	NON	4.3	Juillet 2018	3 militaires	Non déterminant mais favorable aux éléments d'ambiance	
RGARA	SR GRENOBLE	21 av Léon Blum 38100 GRENOBLE	1		OUI	10 utilisations	NON	4.3	Janvier 2018	6 militaires	Atteintes aux infrastructures - Homicide (le logiciel s'est avéré peu utile et son utilisation a très vite été stoppée) - Dossiers stupéfiants (recherches de véhicules voire d'individus liés au trafic)	- Logiciel utile pour exploiter de longues séquences et de gros volumes de vidéos notamment en recherches de véhicules essentiellement - Précaution et quelques réserves sur une utilisation sur des dossiers criminels - Utilisation du logiciel généralement non actée en procédure (considéré comme un outil d'aide pour accélérer l'exploitation)

FORMATION ADMINISTRATIVE DE RATTACHEMENT	NOM DE L'UNITÉ	ADRESSE	NOMBRE DE LICENCES POSSÉDÉES...	...DONT CELLES INCLUANT LA RECONNAISSANCE FACIALE	ENCORE FONCTIONNELLE AU 17/11/2023 (DATE DU MESSAGE DE SUSPENSION) ?	FRÉQUENCE D'UTILISATION DE BRIEFCAM (SUR LES 2 DERNIERES ANNEES)	UTILISATION DE BRIEFCAM ACTÉE EN PROCÉDURE ?	VERSIONS	DATE D'ARRIVÉE DANS LE SERVICE	NOMBRE D'UTILISATEURS DANS L'UNITÉ	EXEMPLE D'AFFAIRES MARQUANTES OÙ BRIEFCAM A ÉTÉ DÉTERMINANT	OBSERVATIONS DIVERSES
COMGENDGF	SR GUYANE	CASERNE LA MADELEINE – 1295 ROUTE DE LA MADELEINE – 97300 CAYENNE	1		OUI	11 utilisations	NON	4.3	Février 2018	10 militaires	Néant	Très importantes saisies de vidéos dans la plupart des enquêtes traitées, toutefois une utilisation relative par manque de connaissance et formation du matériel
RGHF	SR LILLE	201 boulevard de Mons 59650 Villeneuve d'Ascq	1		OUI	4 utilisations	NON	4.3	Février 2018	4 militaires	Pas d'exemple déterminant ; le gain de temps réalisée grâce à l'outil permet simplement d'être plus efficient dans l'enquête.	Utilisation essentiellement pour travailler les différents formats de fichier vidéo et pour gagner du temps en allant à l'essentiel, soit par élimination des images vides soit par sélection des images contenant les objets recherchés. Les images d'intérêt utilisées en procédure étant le résultat d'une recherche humaine au sein de la sélection réalisée par Briefcam, le recours à cet outil n'était pas mentionné en procédure.
RGNA	SR LIMOGES	CASERNE BEAUBLANC - 101 AVENUE MONTJOVIS - 87100 LIMOGES	1		NON	0 utilisation sur 2 ans (en panne depuis environ 2 ans)	NON	4.3	Février 2018	0 militaire	Actuellement 0	Ordi HS
RGARA	SR LYON	Caserne DELFOSSE 2 rue bichat 69002 LYON	1		OUI	25 utilisations	NON	4.3	Mai 2018	15	Meurtre Stup	
RGPACA	SR MARSEILLE	Caserne Donadieu – 171 avenue de Toulon à Marseille 10ème.	1		OUI	10 utilisations	NON	4.3	Février 2018	30	Homicides	Les options de reconnaissance sont les mêmes pour tous les artefacts. Pour exemple, entre une voiture et une personne, les options sont les mêmes. Il n'y a pas d'option de reconnaissance de similitude de visage.
RGGE	SR METZ	Caserne General Radet 2 Rue Albert Bettannier BP 85195 57075 Metz Cedex 03	1		OUI	7 utilisations	NON	4.3	Avril 2018	5 militaires	Aucun dossier marquant. Briefcam est principalement utilisé pour gagner du temps dans l'exploitation des vidéos (vidéosurveillance ou techniques mises en place par nos services)	
RGOCC	SR MONTPELLIER	359 RUE DE FONT-COUVERTE 34056 MONTPELLIER	1		OUI	20 utilisations	NON	4.3	Janvier 2018	10 militaires	Néant	Matériel apprécié des enquêteur – se révèle être une véritable aide à l'enquête
RGGE	SR NANCY	102 avenue du Général Leclerc 54000 NANCY	1		OUI	6 utilisations	NON	4.3	Février 2018	20 militaires		
RGPL	SR NANTES	19 bis rue de la Mitrie 44000 NANTES	1	X	OUI	50aine d'utilisations	NON	5.6	Début 2018, mise à jour mai 2020	8 militaires	Dossier d'homicide	- Gain de temps important dans l'exploitation des vidéos. - La reconnaissance des plaques d'immatriculation a été importante dans différents dossiers.
RGOCC	SR NIMES	56 Rue Sainte Geneviève à Nimes 30000	1		NON	3 utilisations	NON	4.3	Mai 2018	2 militaires	néant	Licence obsolète depuis 2020
ComGend NC	SR NOUMÉA	16 rue Frédéric Surleau – 98800 NOUMÉA	1		OUI	6 utilisations	NON	4.3	Septembre 2018	13 militaires	Meurtre – Viol – Stupéfiants	L'outil Briefcam permet d'isoler plus rapidement les éléments intéressant l'enquête faisant gagner un temps précieux aux enquêteurs
RGCVL	SR ORLEANS	7 boulevard Marie Stuart 45038 ORLEANS Cedex 1	1		NON	0 utilisations sur 2 ans	NON	4.3	Mai 2018	1	0	
COMGENDPF	SR PAPEETE (987)	ILE DE TAHITI CASERNE BRUAT - AVENUE POUVANAA - BP 89 - 98713 PAPEETE CEDEX	1		NON	Ordinateur hs depuis plusieurs années	NON	4.3	Septembre 2018	Actuellement 0		Ordinateur hs depuis plusieurs années
RGIF	SR PARIS	154 BOULEVARD DAVOUT 75020 PARIS	1		NON	2 utilisations	NON	4.3	Janvier 2018	5 militaires	Dossier d'homicide – Aide au visionnage a posteriori de vidéosurveillance sur voie publique sur une plage de plusieurs heures, aux fins de recensement des passages de véhicules en vue de rechercher le déplacement d'un véhicule identifié)	Les séquences recensées via BF ont fait l'objet d'une visualisation et d'une exploitation manuelle de l'enquêteur

FORMATION ADMINISTRATIVE DE RATTACHEMENT	NOM DE L'UNITÉ	ADRESSE	NOMBRE DE LICENCES POSSÉDÉES...	...DONT CELLES INCLUANT LA RECONNAISSANCE FACIALE	ENCORE FONCTIONNELLE AU 17/11/2023 (DATE DU MESSAGE DE SUSPENSION) ?	FRÉQUENCE D'UTILISATION DE BRIEFCAM (SUR LES 2 DERNIERES ANNEES)	UTILISATION DE BRIEFCAM ACTÉE EN PROCÉDURE ?	VERSIONS	DATE D'ARRIVÉE DANS LE SERVICE	NOMBRE D'UTILISATEURS DANS L'UNITÉ	EXEMPLE D'AFFAIRES MARQUANTES OÙ BRIEFCAM A ÉTÉ DÉTERMINANT	OBSERVATIONS DIVERSES
RGNA	SR PAU	4 COURS LEON BERARD	1		OUI	5 utilisations	NON	4.3	Mai 2018	5 militaires	dossier tentative d'enlèvement	
COMGENDGP	SR POINTE-A-PITRE (971)	CASERNE MIQUEL - 97110 POINTE A PITRE	1	X	NON	10 utilisations	NON	5.4	Début 2018, mise à jour juillet 2020	6 militaires		
RGNA	SR POITIERS	CASERNE SOUS LIEUTENANT FERGEAULT - 1 RUE DU PETIT POLYGONE - 86000 POITIERS	1		OUI	10 utilisations	NON	4.3	Mai 2018	1 militaire	Dossiers criminalité organisée – Aide mais utilisation non déterminante	
RGGE	SR REIMS	2A, rue Bertrand De Mun 51100 REIMS	1		NON	30 utilisations	NON	4.3	Avril 2018	10 militaires	Dossiers AAB majoritairement avec gain de temps considérable sur exploitation vidéo-surveillance des communes	Application non fonctionnelle depuis été 2023
RGBRET	SR RENNES	85 BD CLEMENCEAU – BP 33284 35032 RENNES CEDEX	1		OUI	5 utilisations	NON	4.3	Mai 2018	4 militaires		Aucune mention en procédure
RGNORM	SR ROUEN	39 rue Louis Ricard 76000 ROUEN	1		NON	20 utilisations	NON	4.3	Février 2018	2 militaires référents et 7 utilisateurs	Dossier VAMA séquestration	
COMGENDRE	SR SAINT DENIS (974)	8 Route de la Montagne 97400 SAINT DENIS	1		OUI	3	NON	4.3	Janvier 2018	3 militaires		
COMGENDSBSM	SR SAINT MARTIN	80A route de la Savane 97150 SAINT MARTIN	1	X	OUI	10 utilisations	NON	5.4	Octobre 2019	5 militaires	Homicide – Nécessité du logiciel afin de lire des journées de vidéos. Vol avec arme – séquestration – 4 Tera de vidéos surveillances de plusieurs axes routiers afin de déterminer le point de départ des auteurs et l'axe de fuite. Divers vols avec armes de supérettes	
RGGE	SR STRASBOURG	02 rue de Molsheim 67000 STRASBOURG	1		OUI	10 utilisations	NON	4.3	Mars 2018	10 militaires	Aucun exemple de référence. Briefcam est une solution informatique qui permet de traiter des vidéos en gagnant un temps conséquent au regard des nombreuses investigations à conduire au cours de la phase enquête.	
RGOCC	SR TOULOUSE	202 avenue Jean Rieux 31400 Toulouse	1		OUI	15 utilisations	NON	4.3	Janvier 2018	7 militaires	Dossier de règlement de compte, Dossier de vols dans commerce	Dans ces deux dossiers, l'intégration des vidéos a permis une analyse très rapide et un recentrage, soit sur le cheminement du véhicule, soit sur les véhicules utilisés
RGIF	SR VERSAILLES	55 RUE D ANJOU - 78000 VERSAILLES	1		NON	5 utilisations	NON	4.3	février 2018	5 militaires	Dossier de recel (l'utilisation de l'outil a permis de limiter le visionnage des vidéos remises par la ville)	Retrait des images sans mouvement et filtre sur une zone à prendre en compte. La prévisualisation de la vidéo a permis de limiter le temps de visionnage (exclusion de vidéos hors faits recherchés)
GTA	SRTA	73 avenue Charles de Gaulle – 95700 ROISSY EN FRANCE	1		NON	0 au cours des 2 dernières années	NON	4.3	Début 2018, dernière utilisation le 16/05/2018	Actuellement 0		

Source : sous-direction de la police judiciaire de la gendarmerie nationale, retravaillée par la mission

Annexe n° 8 : La reconnaissance faciale dans *BriefCam*

BriefCam **TRANSFORMER LA VIDÉOSURVEILLANCE EN RENSEIGNEMENTS EXPLOITABLES**

6. BriefCam extrait ensuite les caractéristiques uniques du visage, telles que la distance entre les yeux, la largeur du nez et la forme des pommettes, qui sont les identifiants uniques de ce visage, et les code dans un vecteur de caractéristiques qui représente ce visage. Ce vecteur de caractéristiques est extrait à la fois pour les visages figurant sur une liste de surveillance et pour les visages que BriefCam détecte dans les séquences.
7. La dernière phase est la mise en correspondance des vecteurs de caractéristiques, au cours de laquelle deux vecteurs sont comparés à l'aide d'une fonction qui analyse la distance entre les vecteurs et produit un score qui indique approximativement la probabilité que les deux vecteurs de caractéristiques appartiennent à la même personne. Un score de correspondance supérieur à un certain seuil est considéré comme une correspondance positive.

Principaux cas d'utilisation du marché

Les principaux cas d'utilisation de la reconnaissance faciale sur le marché sont le "contrôle d'accès" et "dans la nature".

Le contrôle d'accès signifie que vous souhaitez décider si une personne peut entrer (accéder) dans une zone. Dans ce scénario, la personne s'identifie généralement et la reconnaissance faciale est 1:1 (vérification un pour un), ce qui signifie que chaque visage est comparé à un visage de référence dans un environnement contrôlé, comme dans un aéroport lorsque le contrôle des passeports compare l'image du passeport dans la base de données biométriques avec un scan de la personne qui se trouve devant lui. Dans ce scénario, le taux de précision est très élevé puisque l'algorithme est seulement
comparer un visage à une identité et puisque, dans la plupart des scénarios de contrôle d'accès, la caméra est positionnée de manière idéale et que d'autres paramètres, tels que l'éclairage, sont contrôlés et optimaux.

Les cas d'utilisation "dans la nature" concernent des sujets "non coopératifs" et sont des cas de reconnaissance de visages 1:N (un à plusieurs) qui se produisent dans un environnement non contrôlé. Le 1:N se réfère à une relation de un à plusieurs, ce qui signifie que chaque visage est comparé à de nombreux visages dans l'ensemble de données d'images. Dans ce cas, vous identifiez des personnes sur la base d'une liste de surveillance. Un exemple de ce type de scénario est l'identification de criminels ou de voleurs à l'entrée d'un établissement.

Source : BriefCam « Le livre blanc Reconnaissance des visages » mai 2022 (extraits)

Annexe n° 9 : L'unique mise en œuvre de la fonctionnalité de reconnaissance faciale du logiciel *BriefCam* dans une procédure judiciaire

A la suite des violences urbaines survenues en France du 27 juin au 7 juillet 2023, consécutives au décès à Nanterre du jeune Nahel lors d'un contrôle routier, une enquête judiciaire a été effectuée par une unité de gendarmerie, pour identifier les auteurs de dégradations de la mairie et des bâtiments de la gendarmerie de la commune de Fosses (95).

Dans le cadre de cette enquête, les enquêteurs de la brigade de recherches de Montmorency (95) ont procédé à la saisie de nombreuses images vidéo. Dans un souci de rapidité, les enquêteurs ont demandé le concours du service central du renseignement criminel (SCRC) du pôle judiciaire de la gendarmerie nationale (PJGN), situé à Pontoise.

Compte tenu du volume des flux vidéos à exploiter, l'utilisation du logiciel *Briefcam* a été décidée.

Dans ce contexte exceptionnel, la fonctionnalité *reconnaissance faciale* de ce logiciel a été activée au SCRC, en intégrant dans *Briefcam* des photographies de personnes soupçonnées par les enquêteurs d'avoir participé aux émeutes, issues de diverses sources, dont le traitement des antécédents judiciaires (TAJ).

Les algorithmes de *BriefCam* ont sélectionné deux séquences vidéo où apparaissaient deux personnes dont les photos avaient été ainsi intégrées dans le logiciel.

Dans ces deux séquences vidéo, ces deux personnes étaient bien présentes sur les voies publiques filmées par les caméras de vidéoprotection.

Cependant, les investigations complémentaires menées par les enquêteurs ont exclu leur participation formelle aux dégradations des bâtiments publics.

Elles n'ont donc pas été interpellées ni mentionnées en procédure.

Source : mission