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 acopter 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 Authenticate : 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