NOTE RAPIDE
DE L'INSTITUT PARIS REGION N°833

Trismegist san

PRÉVENTION-SÉCURITÉ
Février 2020 • www.institutparisregion.fr

LA SÉCURITÉ À L'HEURE DE L'INTELLIGENCE ARTIFICIELLE

L'INTELLIGENCE ARTIFICIELLE EST DE PLUS EN PLUS IDENTIFIÉE PAR LES POLITIQUES ET LES INDUSTRIELS COMME UN DOMAINE D'INTÉRÊT MAJEUR POUR LA SÉCURITÉ PUBLIQUE. ON NE PARLE PLUS DE DISPOSITIFS DE VIDÉOSURVEILLANCE MAIS DE « VIDÉOSURVEILLANCE INTELLIGENTE », CE QUI IMPLIQUE LE RECOURS À UN LARGE SPECTRE DE TECHNIQUES DONT CELLE DÉDIÉE À LA RECONNAISSANCE FACIALE. CE N'EST PAS SANS POSER UN ENSEMBLE DE QUESTIONS : QUELLES SONT LES FINALITÉS DES PROJETS INTÉGRANT L'INTELLIGENCE ARTIFICIELLE À DES DISPOSITIFS DE SURVEILLANCE ? QUELS ENJEUX JURIDIQUES, TECHNIQUES ET ÉTHIQUES SOULÈVENT-ILS ?

En France, depuis les années 1990, le déploiement des dispositifs de vidéosurveillance est continu. On estime que plus d'un million de caméras sont actuellement installées dans les espaces publics et les lieux ouverts aux publics. Malgré cette diffusion massive, la vidéosurveillance demeure un sujet controversé. Considérée par d'aucuns comme un outil indispensable de lutte contre la délinquance et en tant que tel, dûment subventionnée, elle fait aussi régulièrement l'objet de réserves, voire de critiques. Le manque d'évaluation institutionnelle et la structuration d'un marché économique autour de son installation amènent à contester son impact préventif et dissuasif. Chercheurs et associations de défense des libertés individuelles, entre autres, l'accusent ainsi d'être inefficace dans la prévention et la lutte contre la délinquance et le terrorisme, et de renforcer une gestion sécuritaire des problèmes sociaux (Mucchielli, 2018 ; Lemaire 2019).

Avec le développement des techniques d'intelligence artificielle, la vidéosurveillance entre dans une nouvelle ère, celle où les images filmées par les caméras de surveillance peuvent être analysées en temps réel par des algorithmes capables d'identifier des individus recherchés ou des situations potentiellement dangereuses ou, du moins, susceptibles d'intéresser les forces de l'ordre. Les images ainsi triées apparaissent alors sous forme d'alertes dans les postes de commandement, où l'opérateur, en fonction de ce que lui propose la machine, n'a plus qu'à valider (ou invalider) le choix de l'algorithme et de prévenir (ou non) les forces de sécurité. Les attentes envers les dispositifs de vidéosurveillance se voient ainsi réaffirmées. Ces systèmes dits « intelligents » se font progressivement une place dans la coproduction de la sécurité quotidienne. Considérés comme « des outils parmi tant d'autres », ils soulèvent, néanmoins, divers enjeux dont ceux relatifs à la protection des libertés individuelles.

L'INSTITUT PARIS REGION

1. Les systèmes biométriques (reconnaissance faciale et digitale) des objets connectés du quotidien se généralisent.

2. En France, plus d'un million de caméras de surveillance sont installées dans les espaces publics et les lieux ouverts aux publics.

3. La police chinoise est l'une des premières à utiliser des dispositifs de reconnaissance faciale dans l'espace public.

4. La « smart city » soulève des questions concernant la protection des données personnelles et des libertés individuelles.

LE CADRE LÉGAL ACTUEL

En France, la loi informatique et libertés de 1978 sert toujours de cadre de référence pour l'installation de caméras de surveillance et la protection des données à caractère personnel[1]. En mai 2018, la mise en œuvre du Règlement général de protection des données (RGPD) est venue renforcer les tendances initiées par la loi de 1978. Le traitement de données à caractère personnel n'y est pas interdit, mais se doit d'être conforme. La protection des personnes physiques à l'égard des traitements de données est également entérinée. Les traitements mis en œuvre pour assurer la sûreté de l'État ou encore la défense nationale ne relèvent pas du champ d'application de l'Union européenne (ni du RGPD) et sont régis par les dispositions de la directive n°2016/680 du 27 avril 2016, dite directive « Police-Justice ». Concernant les traitements portant sur des données sensibles (comprenant les données biométriques), la directive prévoit qu'ils ne peuvent être autorisés qu'en cas de nécessité absolue (article 10).

LA DÉTECTION DES COMPORTEMENTS JUGÉS « ANORMAUX »

Dans le contexte actuel de lutte anti-terroriste, l'intelligence artificielle est développée dans l'objectif de cibler les comportements qui pourraient prévenir le passage à l'acte d'un éventuel délinquant ou terroriste. En Île-de-France, plusieurs projets en cours vont dans ce sens.

Les espaces de transport : terrain d'expérimentation

La RATP est régulièrement sollicitée par les industriels pour participer à des programmes de recherche-action visant à perfectionner la technicité des algorithmes. Elle bénéficie à la fois d'un réseau souterrain spécifique et d'un important parc de caméras de surveillance : plus de 50 000. Depuis peu, elle a créé un laboratoire dédié à l'intelligence artificielle à la station Châtelet-Les Halles. Pour le moment, les expérimentations qui y sont menées servent à valider des technologies et n'ont pas de retombées opérationnelles directes. La RATP y a déjà expérimenté des algorithmes visant à détecter des situations problématiques, telles que : les intrusions sous tunnel, le maraudage[2], les rixes et les objets abandonnés. Les résultats ont été plus ou moins mitigés en fonction des scénarios, comme pour le maraudage, où l'expérimentation n'a pas donné de résultats probants, l'algorithme s'étant heurté aux usagers qui attendent un rendez-vous ou qui cherchent simplement leur itinéraire.

Ce sont principalement des raisons techniques qui expliquent les « faux-positifs ». L'ancienneté du parc de caméras (98 % sont analogiques) compromet également les résultats dans ce domaine. Les images sont de qualité médiocre et les angles de vue des caméras rendent difficile le fonctionnement des algorithmes. En outre, l'environnement spécifique du métro parisien (souterrain, vibrations récurrentes, poussières, flux quotidiens importants de voyageurs, etc.), sont autant d'éléments qui compliquent leur tâche. Pour autant, le transporteur, conscient de ces limites techniques, s'investit toujours davantage dans ce domaine. Depuis peu, la RATP enregistre les images filmées quotidiennement, en floutant les visages des usagers, pour créer une base d'apprentissage pour les prochains algorithmes et les entraîner aux conditions réelles de ses espaces (luminosité, vibrations, flux aux heures de pointe, notamment).

Des collectivités locales proactives

Les collectivités locales s'intéressent aussi à la détection des comportements. Le syndicat mixte Seine-et-Yvelines Numérique, porté par les Yvelines et les Hauts-de-Seine, œuvre, entre autres, au déploiement de dispositifs de vidéosurveillance sur son territoire[3]. L'ensemble des images filmées a vocation à être directement envoyé au centre départemental de supervision des images (CDSI), où un opérateur est présent 24 heures sur 24. L'innovation repose sur l'utilisation de plusieurs algorithmes pour aider l'opérateur à repérer les situations qui pourraient être « anormales »[4]. Pour le moment, le projet se heurte à des limites juridiques (que le syndicat mixte ne se cache pas de vouloir faire évoluer) puisque les images filmées par les municipalités ne peuvent pas être traitées par des agents relevant du département. Il s'agit néanmoins d'un projet d'équipement d'ampleur en matière de vidéosurveillance dite « intelligente ».

Récemment, la ville de Saint-Étienne a souhaité expérimenter un projet d'audiosurveillance. Via des capteurs sonores installés dans un quartier, le projet visait à saisir les sons et à repérer les bruits considérés comme « suspects » : cris, verre brisé, klaxons, crépitements, coups de feu, etc. Un algorithme les comparait ensuite avec des modèles préenregistrés en vue de déclencher ou non une intervention des forces de sécurité. Cette expérimentation prévoyait également de coupler ce système de prises de sons aux images filmées par les caméras de surveillance. La Cnil[5] s'est opposée à ce système d'écoute sur l'espace public en estimant qu'à défaut de base légale spécifique, le traitement de données à caractère personnel (en l'occurence la voix pouvant permettre ici l'identification) est illégal et en a interdit son expérimentation.

Par-delà la conformité juridique, l'ensemble de ces démarches soulève des questions éthiques : des algorithmes peuvent-ils participer à interpréter un comportement ou des sons jugés « anormaux » ? Plus largement, qu'est-ce que la normalité au sein des espaces publics ?

LA RECONNAISSANCE FACIALE : DU MYTHE À LA RÉALITÉ

Si elle a pendant longtemps été assimilée à un sujet de science-fiction, la reconnaissance faciale fait aujourd'hui plus que jamais l'actualité. Techniquement bien mieux maîtrisée, elle est au cœur des discours concernant l'intelligence artificielle. Associée à des enjeux de sécurité et d'ordre public, elle soulève cependant de nombreuses craintes.

Des dispositifs de ce type sont déjà utilisés en France. En 2018, les aéroports de Roissy et Orly se sont équipés de sas de reconnaissance faciale pour, entre autres, réduire les temps d'attente provoqués par les mesures de sécurité et de contrôle des passagers. Ces sas ont été mis en place pour récupérer les données biométriques inscrites au sein des puces électroniques des passeports (qui comprennent la photographie et deux empreintes digitales de son détenteur). Une fois le sas ouvert, une caméra vérifie la correspondance entre le visage qu'elle filme et les données du passeport.

Du côté du ministère de l'Intérieur, le sujet de la reconnaissance faciale est peu documenté. Une absence de transparence qui tend à renforcer les inquiétudes et les suspicions à l'égard de cette technologie. Pour le moment, les forces de l'ordre peuvent recourir à des systèmes de reconnaissance faciale pour toutes les personnes enregistrées dans le fichier TAJ - traitement des antécédents judiciaires[6]. Ce fichier comprendrait entre 7 et 8 millions de photographies de face. Selon certaines sources, en pratique, il n'est pas rare que policiers et gendarmes disent pouvoir faire « de la comparaison faciale », c'est-à-dire confronter une photo ou une image prise par une caméra de surveillance avec la base photographique enregistrée dans le fichier TAJ[7]. Cependant, on ne peut pas dire si cette pratique est complètement généralisée et à quel niveau hiérarchique les agents y ont recours. Ces derniers mois, les annonces d'expérimentation de dispositifs de reconnaissance faciale se sont multipliées.

En février 2019, la ville de Nice a pour la première fois expérimenté un dispositif de reconnaissance faciale sur la voie publique lors de son carnaval annuel. Durant deux jours, des personnes volontaires ont ainsi été identifiées dans la foule par le biais des caméras de surveillance et à partir d'une photographie enregistrée au préalable. Bien que la Cnil ait été avertie, elle a publiquement regretté avoir été associée trop peu de temps avant le début de cette expérimentation. En octobre dernier, c'est le projet de « portique virtuel » initié par la région Sud (ex-Paca) qui a fait parler de lui. Deux lycées situés à Nice et Marseille devaient être équipés de sas de reconnaissance faciale dans le but de fluidifier et de sécuriser les accès de ces établissements. La Cnil a rejeté l'expérimentation, considérant le dispositif trop intrusif et présentant des risques d'atteintes à la vie privée et aux libertés individuelles de personnes essentiellement mineures. Dans sa note, elle attire l'attention sur la disproportion des réponses envisagées par rapport aux objectifs initiaux et recommande, pour optimiser la gestion des entrées, un contrôle par badge.

Ces derniers mois, la Cnil s'est positionnée comme la seule autorité administrative compétente à faire respecter le cadre légal, faute d'une réglementation adaptée et spécifique à la reconnaissance faciale et au traitement de données biométriques. À ce jour, le sujet divise. De plus en plus d'institutions (politiques, industriels, transporteurs, etc.) appellent à élaborer un cadre légal sur ce sujet pour mieux multiplier les expérimentations. En revanche, nombreuses sont aussi les organisations à demander à « interdire tout usage sécuritaire de dispositifs de reconnaissance faciale actuels ou futurs »[8].

DÉFINITIONS

- **Algorithme :** Description d'une suite finie et non ambiguë d'étapes ou d'instructions permettant d'obtenir un résultat à partir d'éléments fournis en entrée.
- **Biométrie :** Regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.).
- **Intelligence artificielle :** Théories et techniques « consistant à faire faire à des machines ce que l'homme ferait moyennant une certaine intelligence » (Marvin Minsky). On distingue IA faible (IA capable de simuler l'intelligence humaine pour une tâche bien déterminée) et IA forte (IA générique et autonome qui pourrait appliquer ses capacités à n'importe quel problème, répliquant en cela une caractéristique forte de l'intelligence humaine, soit une forme de « conscience » de la machine).
- **Reconnaissance faciale :** Une technique qui permet à partir des traits de visage :
  - d'authentifier une personne, c'est-à-dire vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès), ou
  - d'identifier une personne c'est-à-dire de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

Source : www.cnil.fr

L'ENJEU SÉCURITAIRE DE LA « SMART CITY »

La « smart city » s'est développée au travers d'un imaginaire, celui d'une ville organisée et contrôlée à partir de capteurs et d'algorithmes, où l'intelligence artificielle permettrait d'anticiper chaque pan de la gestion urbaine. Dans le domaine de la sécurité publique, l'innovation passe, entre autres, par une surveillance accrue des zones potentiellement dangereuses et des individus recherchés, et par l'anticipation et la proactivité des patrouilles sur les territoires. Ce volet sécuritaire, communément admis, pose en réalité question. Que suppose-t-il pour les libertés individuelles et la protection de l'anonymat au sein des espaces publics ? Comment participe-t-il à déterminer les comportements et les usages ? Dans le contexte actuel de lutte anti-terroriste et de maintien de l'ordre renforcé face à des mouvements sociaux réguliers, ces questions doivent être posées et débattues publiquement. C'est ce à quoi la Cnil appelle dans une note publiée en novembre 2019, proposant l'établissement d'un « code de la route » consacré à la reconnaissance faciale[9].

Par ailleurs, la structuration des industriels de ce secteur, l'approche de grands évènements, tels que la Coupe du monde de rugby ou les Jeux olympiques, sont autant d'éléments qui pourraient venir accroître les pressions sur la mise en œuvre de dispositifs de sécurisation. Pour le moment, la reconnaissance faciale ne dispose pas d'un cadre réglementaire propre et spécifique. C'est pourquoi partisans et adversaires perçoivent l'année 2020 comme charnière. ■

Camille Gosselin, urbaniste
mission Prévention sécurité *(Sylvie Scherer, directrice)*

RESSOURCES

- Benbouzid Bilel, « À qui profite le crime ? Le marché de la prédiction du crime aux États-Unis », *La Vie des idées,* 13 septembre 2016.
- Cnil, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle,* décembre 2017.
- Cnil, *Reconnaissance faciale, pour un débat à la hauteur des enjeux,* novembre 2019.
- Fernandez Rodrigez Laura, Elie Mathilde, « La smart city est-elle autoritaire ? », *La Gazette des communes,* publié le 17 septembre 2019.
- Gosselin Camille, *La police prédictive, enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique,* Institut Paris Region, avril 2019.
- Lemaire Élodie, *L'œil sécuritaire, Mythes et réalités de la vidéosurveillance,* Éditions La Découverte, PUF, Paris, 2019.
- Mucchielli Laurent, *Vous êtes filmés, Enquête sur le bluff de la vidéosurveillance,* Armand Collin, Paris 2018.
- Schœnher Dominique, « Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité », *Note du CREOGN,* n° 43, septembre 2019.

1. La loi de 1978 pose notamment certaines obligations pour que l'exploitation des images se fasse dans le respect des libertés individuelles : interdiction de visualisation des espaces privés, limitation de la durée de conservation des images à un mois, possibilité d'accéder aux images par les personnes filmées, obligation d'information du public.
2. Dans le cas présent, la détection du maraudage consiste à ce que l'algorithme repère une personne statique pendant plus de 300 secondes dans un lieu à vocation de passage. En l'occurrence, la RATP a mené cette expérimentation dans la salle d'échanges du RER à la station Les Halles.
3. Pour le département des Yvelines, le programme vise à équiper : 116 collèges, 50 services départementaux d'incendie et de secours (SDIS), 80 bâtiments départementaux et les municipalités qui le désirent en caméras de vidéosurveillance, d'ici la fin de l'année 2020.
4. Certains algorithmes sont ainsi libellés : « flux massif de type panique devant la porte d'entrée », « effondrement de N personnes », « personne au sol inanimée depuis N secondes », « détection de présence sur les toits et terrasses », « circulation rapide dans l'enceinte du collège (moto, quad, 4x4…) », etc.
5. Commission nationale de l'informatique et des libertés.
6. Le fichier TAJ créé par le décret du 4 mai 2012 est le produit de la fusion du Stic – système de traitement de l'information criminelle - (côté police) et du Judex – système judiciaire de documentation et d'exploitation - (côté gendarmerie). Ce fichier contient l'ensemble des informations des personnes mises en cause dans des infractions, auteurs comme complices ainsi que de leurs victimes : nom, domicile, photographie, faits reprochés.
7. La Quadrature du Net, « La reconnaissance faciale des manifestant.e.s est déjà autorisée », 18 novembre 2019.
8. L'Observatoire des libertés numériques, La Quadrature du Net, la Ligue des droits de l'Homme, Amnesty International France, le Syndicat de la magistrature, etc. signent une lettre commune appelant le gouvernement à interdire toute pratique de reconnaissance faciale sécuritaire : « Lettre commune de 80 organisations : interdisez la reconnaissance faciale sécuritaire », 19 décembre 2019.
9. *Cf.* Cnil, « Reconnaissance faciale, pour un débat à la hauteur des enjeux », 15 novembre 2019.

DIRECTEUR DE LA PUBLICATION
Fouad Awada
DIRECTRICE DE LA COMMUNICATION
Sophie Roquelle
MAQUETTE
Jean-Eudes Tilloy
MÉDIATHÈQUE/PHOTOTHÈQUE
Inès Le Meledo, Julie Sarris

FABRICATION
Sylvie Coulomb
RELATIONS PRESSE
Sandrine Kocki
33 (0)1 77 49 75 78

L'Institut Paris Region
15, rue Falguière
75740 Paris Cedex 15
33 (0)1 77 49 77 49

ISSN 1967-2144
ISSN ressource en ligne
2267-4071

www
institutparisregion.fr