LIVRE BLANC POUR L'OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Surveiller les foules

POUR UN ENCADREMENT DES IA « PHYSIOGNOMONIQUES »

[SYNTHÈSE]

Sous la direction de C.Lequesne Roth

Avec les contributions de C.Lequesne Roth et J.Keller

AVRIL 2023

Région Hauts-de-France

OBSERVATOIRE de l'ÉTHIQUE PUBLIQUE

SOUS LA DIRECTION de

Caroline Lequesne – Roth

Maître de conférences HDR en Droit public à l'Université Côte d'Azur, membre du GREDEG (CNRS – UMR 7321)

AVEC LES CONTRIBUTIONS de

Caroline Lequesne – Roth

Maître de conférences HDR en Droit public à l'Université Côte d'Azur, membre du GREDEG (CNRS – UMR 7321)

Jonathan Keller

Ingénieur de recherche (Département SES, Institut Mines Telecom), chef de projet du Projet Living Lab 5G mené en partenariat avec la SNCF, Nokia et Orange et financé par la Banque Publique d'Investissement (BPI)

EN BREF

Le présent rapport intéresse le recours aux technologies d'identification par les forces de police dans les espaces accessibles au public : reconnaissance faciale, vidéosurveillance intelligente, systèmes de police « prédictive ». Un des points de convergence technologique tient dans la mobilisation de techniques dites d'IA « physiognomoniques ». La physiognomonie promet de déduire des caractéristiques physiques d'une personne, certains traits de caractère. Cette pseudo science - héritée de l'Antiquité et promue de manière controversée au 19e siècle - connaît aujourd'hui une résurgence au travers du déploiement de l'intelligence artificielle. Nous désignons comme IA physiognomoniques les systèmes développés au service de l'identification des personnes dangereuses, au départ du gabarit d'un visage (reconnaissance faciale) ou du gabarit standard d'une personne considérée comme dangereuse (reconnaissance comportementale et émotionnelle). La présente étude dresse un état des lieux des usages de ces technologies, en analyse les risques et le régime juridique applicable, puis formule, en conclusion, des propositions visant à en combler les lacunes. Pour renforcer la démocratie technologique, l'étude plaide en faveur d'une stricte restriction des usages et de l'adoption d'un régime de redevabilité adapté.

REMERCIEMENTS

Les auteurs tiennent à remercier l'équipe de l'Observatoire de l'Ethique Publique pour son écoute, les échanges qui ont entouré la réalisation du présent Libre Blanc et le travail éditorial réalisé.

L'encadrement des usages des technologies d'identification alimente l'actualité sociale et juridique depuis plus de deux ans : de la reconnaissance faciale à la vidéosurveillance, la production de rapports et de propositions en écho à la dynamique européenne en témoignent. Il est important de souligner que le droit peut et le législateur doit intervenir. Il en va de la sécurité juridique, et plus largement, de la démocratie. La juridicisation des enjeux éthiques apparaît en outre indispensable pour éviter l'instrumentalisation des chartes éthiques et autres « bonnes pratiques ». L'histoire récente des technologies témoigne de ces dérives : celles-ci induisent un biais d'acceptabilité, qui pourrait conduire à desserrer la contrainte réglementaire et institutionnaliser, in fine, des pratiques démocratiquement contestables.

La présente étude a permis de dresser plusieurs constats :

- Les IA d'identification dites « IA physiognomoniques » (reconnaissance faciale, émotionnelle et comportementale) ont fait l'objet de nombreux travaux scientifiques et suscitent un intérêt accru de la part des forces de l'ordre ;

- En parallèle, elles continuent à alimenter les craintes du public au regard des risques d'atteintes aux droits fondamentaux auxquelles elles exposent les personnes concernées : risque d'atteinte à la vie privée, à la liberté d'expression, d'association, d'aller et venir. Les risques sont d'autant plus signifiants que ces systèmes procèdent à des traitements de données sensibles – les données biométriques – qui se caractérisent par leur immuabilité. Le vol de données biométriques ouvre la voie à une usurpation d'identité, qui offre peu de solutions (contrairement au vol de codes d'accès). Les risques inhérents à ces technologies se posent ainsi, également, sur le terrain de la sécurité et de la souveraineté des données.

- En termes de déploiement, l'offre industrielle ne rencontre pas les attentes du secteur public de la surveillance en raison d'un cadre juridique et procédural encore incertain. En sus de fondements légaux lacunaires, l'analyse révèle que le régime de redevabilité n'est pas adapté aux risques identifiés.

- Les propositions légales en cours (Artificial Intelligence Act à l'échelon européen et Loi d'expérimentation pour les JO 2024 à l'échelon national) apportent de premiers éléments de réponse sans toutefois résoudre l'ensemble des difficultés identifiées :
    - L'AIA offre une base légale au déploiement des technologies d'identification à des fins de surveillance dans les espaces accessibles public ; la proposition renvoie toutefois la balle aux législateurs pour élaborer les procédures de déploiement indispensables au respect des garanties constitutionnelles et conventionnelles ;
    - La loi d'expérimentation pose les premiers jalons de ces procédures pour la vidéosurveillance dite intelligente. Elle peine toutefois à identifier les risques et n'instaure aucun contrepouvoir substantiel, ceux-ci étant concentrés dans les mains de l'exécutif.

Les présentes recommandations visent à compléter l'arsenal législatif pour renforcer les conditions de la démocratie technologique.

1. Limiter strictement les usages de l'IA physiognomonique

Eu égard aux risques que ces technologies soulèvent en termes de sécurité et de droits fondamentaux (surveillance de masse), leur usage par les forces de l'ordre doit être substantiellement restreint. Dans le prolongement de l'AIA (article 5), nous plaidons pour le maintien strict de leur interdiction à des fins d'identification **en temps réel dans les espaces accessibles au public.** Le champ de ces **exceptions** doit aussi être strictement limité et circonscrit. L'AIA paraît à cet égard trop large et réduit substantiellement la portée de l'interdiction.

Concernant la reconnaissance faciale, les exceptions renvoient aux infractions pénales visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil qui intègrent, notamment, des infractions de nature économique. Celles-ci nous semblent devoir être écartées et concerner uniquement les **crimes** menaçants - ou portant atteinte - à l'intégrité physique des personnes. Une nouvelle fois, au regard des risques que comporte la technologie,

la proportionnalité des moyens impose que l'usage de la reconnaissance faciale ne puisse faire l'objet d'aucune autre alternative.

Comme précédemment souligné, les distinctions opérées entre authentification et identification apparaissent justifiées au regard des risques encourus. Les opérations d'identification doivent faire l'objet d'un encadrement plus strict.

L'exigence de proportionnalité exclut ainsi l'usage de la reconnaissance faciale à des fins d'indentification, lequel doit formellement être interdit en certains domaines à l'instar des écoles, des établissements d'enseignement, et sur les lieux de travail.

En outre, le respect des principes de proportionnalité et de nécessité impose que le recours à l'identification faciale automatisée soit strictement circonscrit (notamment dans le temps et l'espace) et subordonné à des circonstances exceptionnelles (risques pour la sécurité et l'intégrité des personnes).

2. Identifier les autorités compétentes

La question des autorités pertinentes et de leurs moyens constitue un élément essentiel du régime de redevabilité qui sera mis en place (de son efficacité et de son effectivité).

La proposition de règlement européen sur l'intelligence artificielle a initié un débat, déjà entamé par la doctrine, concernant les autorités de contrôle en matière des systèmes intelligents. La proposition prévoit en effet, dans son modèle de gouvernance, l'instauration d'autorités nationales dédiées. Au regard de l'articulation que supposera le droit de la protection des données à caractère personnelle et ce droit en cours d'adoption, la Commission Nationale Informatique et Libertés (CNIL) semble désignée pour assurer les missions de d'accréditation et de contrôle. Elle s'est d'ailleurs prononcée en ce sens dans le cadre d'un avis conjoint avec ses homologues européens.

Cette proposition nous semble bienvenue sous réserve que la CNIL soit dotée des moyens financiers, humains et techniques supplémentaires pour assurer ces nouvelles missions. La

question des contrôles conjoints entre autorités - combinant par exemple, du contrôle technique pur à des contrôles juridiques - devra en outre être soulevée et clairement établie.

En ce qui concerne l'usage des technologies d'identification par les forces de l'ordre, il apparaît nécessaire de concevoir différents contrôles en fonction de deux paramètres : la temporalité du déploiement (autorisation/contrôle a posteriori des usages) et les pouvoirs de police concernés (police administrative/police judiciaire).

Dans le cadre préventif (police administrative), les autorisations de déploiement - qui concerneraient la surveillance exceptionnelle d'un espace accessible au public - pourrait être délivrée par la CNIL. Celle-ci veillerait également au respect du protocole défini, et contrôlerait a posteriori les usages mis en œuvre. Il serait, à cet égard, souhaitable que soit distingués en son sein les agents (voire les cellules), dédiés aux accréditations de ceux dévolus au contrôle a posteriori.

Dans le cadre répressif (police judiciaire), et conformément au droit de la procédure pénale, le pouvoir d'autorisation devrait être dévolu au juge judiciaire.

En parallèle, il apparaît aujourd'hui indispensable de faire évoluer les contrôles internes des agents à l'aune de l'évolution de l'équipement technologique des forces de l'ordre. Au-delà même de la reconnaissance faciale, l'introduction d'outils d'intelligence artificielle (de type police prédictive) appelle une vigilance particulière concernant la formation des agents dépositaires de l'ordre public, leur habilitation à les utiliser et le contrôle de leur pratique.

Le législateur pourrait à cet effet faire preuve d'innovation en s'appuyant sur les structures existantes. Pourrait ainsi être instituées, au sein de l'Inspection Générale de la Police Nationale (IGPN) et l'Inspection Générale de la Gendarmerie Nationale (IGGN) des cellules « Tech », composées d'ingénieurs et de juristes, chargées de conduire des missions d'audit.

3. Autoriser et contrôler

Dans la perspective de l'instauration d'un régime pérenne, nous plaidons pour l'instauration d'un régime d'autorisation préalable « bicéphale » en fonction des pouvoirs de police concernés (police administrative/police judiciaire) et un **régime de contrôle a posteriori** veillant à la conformité des usages.

Conformément à la jurisprudence constitutionnelle et européenne, tout déploiement de la technologie à des fins d'identification devra être **limité :**

- Dans le cadre préventif (en temps réel): dans le temps (événement présentant un risque pour le maintien de l'ordre), dans l'espace (périmètre concerné) et désigner expressément les personnes habilitées à son emploi.
- Dans le cadre répressif (reconnaissance a posteriori), à la demande formulée auprès du juge judiciaire.

Nous plaidons, à cet égard, pour l'assimilation des recherches par reconnaissance faciale à des **actes d'information ou d'instruction.**

Outre les principes de nécessité et proportionnalité, et dans la ligne de l'AIA (article 5), l'autorisation devra nécessairement être subordonnée au déploiement d'un **protocole dédié** précisant les garanties adoptées et adaptées concernant notamment :

- L'information du public ;
- La minimisation des données (données conservées, temps de conservation) ;
- La supervision humaine (système de vérification des résultats engendrés par les systèmes) ;
- La sécurité des données (l'usage de solutions commerciales telles que celles offerte par Clearview, outre son caractère illégal, est considéré comme techniquement risqué) ;
- La traçabilité des données ;
- Les modalités des processus d'évaluation et les exigences de compte rendu ex-post (relatives, notamment, aux erreurs techniques et aux biais comme demandé par la CNIL à l'issue de l'expérimentation niçoise).
- Le protocole devra également préciser les finalités du traitement, les dates de déploiement du dispositif et les personnes habilitées à solliciter des requêtes.
- La désignation des agents compétents, sur la base d'une formation adaptée.

Ces éléments apparaissent d'autant plus essentiels que l'AIA dessine une délégation normative au bénéfice du secteur privé au travers d'un système de certification contestable. En effet, la procédure de mise en conformité des systèmes prévue à l'article 43-1 de l'AIA - dont relèveraient les systèmes d'identification faciale compris comme « systèmes à haut risque » - sera dans une large mesure dévolue à ces organismes. Il appartiendra(it) à ces derniers d'établir la méthodologie et les normes d'évaluation. Ce modèle confère(rait) un rôle d'importance majeure à des acteurs privés (régulation de l'accès au marché et normes de conformité). L'imposition de protocoles et d'audits propres à l'administration publique apparaît, à cet égard, d'autant plus décisive.

4. Reconnaître la normativité des actes numériques

La normativité des usages – des actes – juridiques n'est aujourd'hui nullement prise en compte. [Conseil constitutionnel, 12 juin 2018]. Il est impératif que la normativité des recherches effectuées avec ces logiciels soit reconnue. Le rapport de contrôle de l'Organe belge de contrôle de l'information policière déjà mentionné révèle à ce titre des pratiques préoccupantes du point de vue de l'état de droit. Il relève que l'usage des outils de reconnaissance faciale est apparenté, au sein des forces de police belge, à une recherche sur un moteur Internet. Ces traitements ont souvent lieu pendant la phase préalable à une ouverture ou une instruction et ne sont « nulle part saisis ni journalisés dans les banques de données policières existantes »[1]. Ces traitements biométriques sont dès lors réalisés en dessous des « radars juridiques » et donc des impératifs démocratiques.

Il nous paraît aussi indispensable que l'usage de la reconnaissance faciale soit assimilé, dans le cadre des procédures pénales, à des actes d'information ou d'instruction, et soumis à leur même régime.

5. Renforcer le devoir d'information

Par ailleurs, et dans le même sens, les forces de l'ordre devraient être tenues à un devoir d'information à l'égard des personnes concernées dès lors qu'elles font usage de ces

[1] *Rapport DIO21006, Février 2022.*

technologies. Pour être effective, l'information doit être multi-niveaux et multi-supports. Lors des expérimentations conduites au Royaume-Uni dans les espaces accessibles au public, les organisations non gouvernementales ont mis en évidence qu'en dépit des efforts des autorités, la signalétique était insuffisante pour permettre aux personnes concernées d'exercer leurs droits (alternative quand les expériences étaient fondées sur le consentement), et de comprendre les enjeux. La Cour d'appel qui s'est prononcée sur l'usage de la reconnaissance faciale par la police du Pays de Galles a confirmé cette analyse : le triple dispositif déployé (informations sur les réseaux sociaux, les véhicules de police et distribution de flyers) ne suffisait pas à prévenir les atteintes au droit de la vie privé constatées ([2020] EWCA Civ 1058 §20). Le devoir d'information doit aussi faire l'objet d'un protocole (déployé par l'autorité de contrôle ou en collaboration avec celle-ci dans le cadre des expérimentations). À défaut, le risque est celui d'une « banalisation » de ce droit au mépris de l'acceptabilité sociale à laquelle il doit contribuer.

6. Approfondir les analyses d'impact

Nos analyses ont mis en évidence les lacunes liées à aux analyses d'impact. Elles résultent de la conjonction entre l'absence d'obligation expresse et le caractère discrétionnaire de la méthode (l'opportunité de leur réalisation et l'identification des risques relève de l'appréciation de seul responsable de traitement).

Pour renforcer la transparence des usages, le législateur devrait consacrer l'obligation de publier l'analyse d'impact relative à la protection des données (AIPD) réalisée en amont du déploiement de ces technologies. Tout utilisateur d'un système d'identification dans les espaces accessibles au public devrait être tenu de soumettre son AIPD à la CNIL en amont de tout déploiement, pour lui permettre un contrôle effectif.

A minima, le responsable du traitement devrait être tenu de publier un résumé clair, accessible aux néophytes. Celui-ci comprendrait, sous une forme intelligible :

- l'ensemble des décisions ou des situations faisant l'objet d'un traitement automatisé,
- les critères intervenant dans une décision,
- les informations sur les données utilisées,
- une description de la méthode utilisée pour la collecte de données.

Pour préserver certains secrets des affaires, ce résumé pourrait être expurgé de tous les éléments techniques pour se concentrer uniquement sur le type de données collectées et leur traitement précis.

Cette communication offrirait tant au public concerné qu'à la CNIL un moyen de contrôle supplémentaire.

Nous encourageons également le législateur à rendre cette consultation juridique préalable de l'utilisateur d'une IA physiognomoniques payante, pour permettre à la CNIL de se doter les moyens humains et techniques pour exercer ce contrôle.

Nous invitons parallèlement le législateur à préciser la méthodologie des AIPD relatives aux IA physiognomoniques de la façon suivante :

- L'analyse devra porter principalement sur la vraisemblance des risques en répondant aux exigences de sûreté, de sécurité et de robustesse dès la conception ;
- L'examen devra effectuer une analyse d'impact s'assurant que certaines caractéristiques telles que le genre ou la couleur de peau sont exclues, pour éviter les discriminations illégales ;
- L'analyse devra notamment identifier les impacts négatifs potentiels du système de traitement sur les droits de l'homme en documentant toutes les évolutions du modèle ;
- L'analyse devra être contrôlée, à l'instar de ce qui est fait dans le domaine financier, par deux entités privées concurrentes pour s'assurer de la sincérité des résultats ;
- L'analyse réalisée devra enfin voir son résumé être communiqué soit au journal officiel, soit dans un bulletin municipal officiel.

7. S'interroger quant au régime de consentement

Force est de constater une différence d'acceptabilité et de régime entre les usages individuels des IA d'identification (déverouillage des smart phones, entretien d'embauche) et leurs usages dans les espaces accessibles au public ; cela tient notamment aux finalités distinctes des traitements (surveillance individuelle v./surveillance publique). Aussi, les fondements juridiques des traitements ne sont - et ne peuvent pas être - les mêmes.

Pour autant, il est vrai que les deux régimes entrent en collision : comment justifier que la reconnaissance faciale soit admise pour déverrouiller nos téléphones et non pour faciliter la recherche d'un enfant perdu dans des conditions très restrictives ?

Cet écueil appelle à penser de concert les deux régimes.

Au regard des risques déjà évoqués, le régime de consentement (qui caractérise principalement les usages privés) doit être mis en cause dans certains cas, comme dans le cadre professionnel pour prévenir des rapports de force inégaux et des usages disproportionnés. En parallèle, le régime public doit être conçu et construit autour d'usages restreints apportant de fortes garanties en matière de contrôle et de redevabilité. L'acceptabilité sociale sera en grande partie fonction de celles-ci : la transparence des autorités, l'information du public et les contrôles établis apparaissent à cet égard indispensable.

CRÉDITS

Mise en page : Anaïs Rebuccini (Observatoire de l'éthique publique)

Images : sauf mention contraire, toutes les images utilisées dans ce document sont libres de droits et diffusées sous licence adobe stock

LIVRE BLANC POUR L'OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Surveiller les foules

POUR UN ENCADREMENT DES IA « PHYSIOGNOMONIQUES »

https://www.observatoireethiquepublique.com/
IEP de Lille – 9 Rue Auguste Angelliers – 59000 LILLE
E-mail : contact@observatoire-ethique-publique.com
Twitter : @ObservatoireEP
LinkendIn : L'Observatoire de l'Ethique Publique