

La reconnaissance faciale en procès !

“Dire que vous ne vous souciez pas de la vie privée parce que vous n’avez rien à cacher revient à dire que vous ne vous souciez pas de la liberté d’expression parce que vous n’avez rien à dire. Mais le fait est que, même si vous n’utilisez pas un droit donné à cet instant précis, d’autres personnes le font. Dire qu’on ne se soucie pas d’un droit parce qu’on ne l’utilise pas personnellement est la chose la plus antisociale que l’on puisse dire. Ce que cela signifie, c’est “Je me fiche des autres”. En particulier lorsque cela est dit par quelqu’un qui occupe une position de privilège. Si vous êtes un homme riche, âgé et blanc au sommet de l’échelle sociale, vous n’avez pas à vous soucier des lois, à vous soucier du droit, car la société est organisée pour protéger vos intérêts. Ce sont toujours les minorités qui doivent faire face aux risques les plus élevés.”
Edward Snowden, extrait du documentaire « Nothing to hide » 2017.¹

Testés sans autorisation à l’aéroport de Zaventem ou encore à la suite de réunions Interpol, les autorités policières n’ont manifestement pas attendu le feu vert du parlement pour utiliser les logiciels de reconnaissance faciale déjà à leur disposition. En effet, l’espace public regorge de caméras de vidéosurveillance et le renouvellement du matériel et des contrats emporte de plus en plus l’acquisition d’un logiciel d’analyse biométrique. Sans cadre légal, l’usage de la reconnaissance faciale en Belgique est illégal. Et il doit le rester !

En 2023, la coalition « Protect My Face » présentait une pétition de plus de 1000 signatures de citoyen-ne-s bruxellois-es au Parlement régional lui demandant de prendre une résolution pour l’interdiction de l’usage de la reconnaissance faciale dans l’espace public de la capitale.² Ce processus a malheureusement été reporté à la législation suivante et le résultat des élections de 2024 laisse craindre que le débat démocratique n’ait jamais lieu. La volonté politique ne laisse aucun doute. Les médias ne cessent de faire écho aux propos de (futur-es) dirigeant-es politiques affirmant leur volonté d’utiliser la reconnaissance faciale. De quoi faire oublier qu’aucun débat sur le sujet n’a même été entamé.

DES RISQUES SOUS-ESTIMÉS

Une série des questions que posent l’usage par les autorités de la reconnaissance faciale dans l’espace public recoupe celles qu’interroge déjà la vidéosurveillance : impacts sur la liberté de circuler dans l’espace public, sur la vie privée, sur les possibilités de se rassembler et de manifester ou d’exprimer des opinions ou convictions, contrôle social et surveillance continue. Les choix politiques ont fait pencher la balance en faveur du déploiement d’un parc de caméras dont le nombre ne cesse de croître.³ Tout comme l’accoutumance à cohabiter avec ces yeux étatiques et une certaine auto-censure des comportements humains en leur présence.

¹ *Nothing to Hide* est un documentaire franco-allemand de Marc Meillassoux et Mihaela Gladovic, qui s’intéresse aux effets de la surveillance de masse sur les individus et la société. (Disponible en ligne.)

² À ce sujet, voir : Aline Wavreille, *Reconnaissance faciale : souriez, vous êtes filmé-es... et identifié-es*, La Chronique, 203, 4-6, <https://www.liguedh.be/chronique-203-ces-technologies-qui-nous-veulent-du-bien/>

³ À ce sujet, voir : Corentin Debailleul, *Vidéosurveillance à Bruxelles : installer des caméras, mais pourquoi ?*, La Chronique, 203, 11-13, <https://www.liguedh.be/chronique-203-ces-technologies-qui-nous-veulent-du-bien/>

Or, la reconnaissance faciale vient ajouter une couche de risques. Car l'identification biométrique qu'elle se propose de réaliser implique – en plus des caméras capturant des images dans l'espace public et des logiciels d'analyse de celles-ci – l'existence de bases de données de visages avec lesquelles comparer ces images. Outre les innombrables bases de données policières déjà constituées⁴ et l'opacité presque totale qui les entoure⁵, les données biométriques de nos visages, c'est-à-dire le résultat mathématique du calcul des caractéristiques uniques de nos faciès, viendraient constituer de nouvelles bases de données massives qui répertorieraient toute la population⁶. Les systèmes informatiques étant intrinsèquement vulnérables et les interventions humaines non-négligeables, le risque n'est pas inexistant que ces données nous échappent. Les conséquences, elles, sont irrémédiables : on peut changer son mot de passe, pas son visage.

LA POLITIQUE DU « PIED DANS LA PORTE »

Les caméras de vidéosurveillance parsemant nos rues, leur prolifération n'informe pas encore sur les logiciels traitant les flux d'images. C'est pourquoi, depuis 2022, la LDH mène une vaste campagne de demande d'accès aux informations et aux documents administratifs relatifs à l'installation de dispositifs de surveillance de l'espace public par les autorités locales.⁷ S'il ne fait désormais plus aucun doute que le logiciel israélien BriefCam a su se frayer une petite place de favori au sein des marchés publics belges, reste la question de savoir si, en l'absence d'un cadre légal l'autorisant, la tentation d'utiliser la reconnaissance faciale est trop forte. Une récente affirmation du président de l'Organe de l'information policière vient de le confirmer lors d'une interview pour SudInfo⁸ : « *Notre organe de contrôle accepte que les policiers utilisent ce logiciel de reconnaissance faciale mais dans un cadre strict : uniquement dans le cadre d'une enquête précise où il s'agit de reconnaître le visage d'un suspect, en le comparant aux photos qui sont déjà dans les bases de données de la police, à savoir les photos de suspects et de condamnés* ». Sous couvert de quelle disposition légale ? Rien n'est dit à ce sujet.⁹ Il y a donc fort à penser que le cadre légal attendu en Belgique en réception du règlement européen sur l'intelligence artificielle¹⁰ ne viendra que légitimer des pratiques déjà largement répandues.

UN CONTEXTE GLOBAL DE PLUS EN PLUS CONTRÔLANT ET RÉPRESSIF

C'est évidemment le contexte dans lequel les choix politiques – technologues – sont posés qui doit nous alarmer. Le déploiement des outils et technologies de surveillance s'insère logiquement dans un continuum où l'action étatique tend vers toujours plus de contrôle, la politique criminelle vers plus de répression et la politique aux frontières de l'Europe plus inhumaine. Dans l'objectif de lutter contre les demandes d'asile multiples, ce sont désormais les images faciales des personnes introduisant des demandes d'asile qui sont compilées dans la base de données EURODAC, en plus de leurs empreintes digitales.

4 À ce sujet, voir l'enquête du journal Médor sur l'Hypersurveillance policière. <https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/>

5 Voir notamment ce communiqué de la LDH : « *Accès aux bases de données policières : la Cour de justice de l'Union européenne pousse la Belgique à réformer sa loi* », novembre 2023 : <https://www.liguedh.be/acces-aux-bases-de-donnees-policieres-la-cour-de-justice-de-lunion-europeenne-pousse-la-belgique-a-reformer-sa-loi/>

6 Écoutez la série « *Fuyez, vous êtes identifié-es...* » du podcast de la LDH *De quels droits (on se chauffe) ?* <https://www.liguedh.be/podcast/podcast-fuyez-vous-etes-identifie%c2%b7es/>

7 Voir ce communiqué de la LDH : « *Plus de transparence sur la vidéosurveillance* », mars 2022, <https://www.liguedh.be/plus-de-transparence-sur-la-vidEOSurveillance/>

8 Voir : *Comme au procès Pélicot, la police belge utilise aussi un logiciel de reconnaissance faciale* : « *Les policiers peuvent l'utiliser mais dans un cadre strict* », 10/09/2024, Sudinfo, <https://www.sudinfo.be/id879328/article/2024-09-10/comme-au-proces-pelicot-la-police-belge-utilise-aussi-un-logiciel-de>

9 Pourtant, en 2022, un avis du même Organe affirmait sans détour qu'il y avait un consensus quant à l'inexistence de fondement juridique suffisant pour les finalités de maintien de l'ordre ou répressives. Voir : Avis relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (DA210029), https://www.organedeconrole.be/files/DA210029_Avis_F.pdf, pts 9-10.

10 À ce sujet, voir l'article de Chloé Berthélémy, *Mais que fait l'Europe ?*, p17 de ce numéro.

Dans le désespoir, de nombreuses personnes ont choisi de brûler leurs doigts pour brouiller leurs empreintes et pouvoir réintroduire une demande de régularisation.

La reconnaissance faciale, en tant qu'outil d'identification des individu-es, confère à l'État¹¹ une modalité de preuve dont l'objectivité réputée ou présumée tend à invisibiliser de nombreuses perspectives, dont notamment les effets sociaux et éthiques de la surveillance policière algorithmique. Les préjudices socio-techniques, comme les qualifie la criminologue Rosamunde van Brakel – c'est-à-dire les préjudices causés par une interaction entre la technologie et les structures sociales existantes – doivent faire partie intégrante de la mise en débat.

Les catégories de la population déjà discriminées par les pratiques et traitements policiers et judiciaires se verront nécessairement impactées de façon plus importante par cette couche technologique et le discours qui l'accompagne. Que restera-t-il de la présomption d'innocence face à une identification par reconnaissance faciale ? Quels comportements justifieront, à court ou moyen termes, un usage légalisé de cette technologie ?

D'une manière générale, on observe que les finalités justifiant les mesures de surveillance sont mal définies. Qu'elle soit justifiée par des arguments d'efficacité ("pourquoi s'en priver ?"), par l'opportunisme (événements sportifs de grande ampleur), par le sensationnalisme voire la stratégie du choc (à la suite d'un meurtre sanglant ou d'un attentat, les finalités peuvent ensuite progressivement "glisser", c'est ce qu'on appelle le *function creep*). Ça a été le cas à Bruxelles avec le déploiement de caméras à reconnaissance de plaques d'immatriculation. Initialement annoncée à la suite des attentats de 2015 dans le cadre de mesures antiterroristes, elles servent aujourd'hui autant à la police qu'à Bruxelles fiscalité dans le cadre de la zone "basse émissions" (LEZ), et demain, peut-être, pour instaurer une taxe kilométrique. C'est l'évolution d'une norme d'exception vers une normalisation de l'usage qu'il faut empêcher. Et pour ce faire, la seule voie qui protège réellement des dérives est celle de l'interdiction. A défaut de débat, la reconnaissance faciale en procès !

Sans sursaut démocratique et dans l'hypothèse où le droit belge n'imposerait pas un cadre plus protecteur, défenseurs et défenseuses des droits humains devront envisager de soumettre le texte à l'analyse de la Cour constitutionnelle, juridiction suprême chargée d'exercer le contrôle de conformité des lois avec la Constitution, la Convention européenne des droits de l'homme ou des règles de droit primaire de l'Union européenne. C'est pourquoi, dans le cadre du procès fictif écrit par Sophie Delacolette et la Ligue des droits humains pour le Festival des Libertés, le public sera projeté en 2026 dans une réalité – pas si hypothétique – où une asbl appelée Protect My Face serait amenée à introduire, devant la Cour constitutionnelle, un recours en annulation d'une loi établissant un cadre dans lequel certains usages exceptionnels de la reconnaissance faciale seraient autorisés.

¹¹ A ce sujet, voir l'article de Jérôme Margnys, La vie privée, pour quoi faire ? Exigence démocratique et reconnaissance faciale, dans ce numéro p9.