La Chronique
de la Ligue des droits humains asbl
n°208

Bureau de dépôt : rue des Bogards 19, 1000 Bruxelles - Périodique trimestriel | Éditrice responsable : Sibylle Gioe
53, boulevard Léopold II à 1080 Bruxelles | ldh@liguedh.be | www.liguedh.be | Tél. 02 209 62 80

septembre 2024

LIGUE DES DROITS HUMAINS

N° D'AGRÉMENT P801323

bpost PB-PP BELGIE(N) - BELGIQUE

ON VOUS VOIT !

Le procès de la reconnaissance faciale

SOMMAIRE

Coordination
Margaux Hallot

Comité de rédaction
Emmanuelle de Buisseret Hardy, Margaux Hallot, Jean-Jacques Jespers, Manuel Lambert, Pierre-Arnaud Perrouty, Edgar Szoc, Aline Wavreille

Ont participé à ce numéro
Chloé Berthélémy, Jean-Michel Decroly, Rémy Farge, Jérôme Margnys, Sophie Mercier

Relecture
Karine Garcia, Margaux Hallot, Emmanuelle de Buisseret Hardy, Manuel Lambert, Aline Wavreille

Illustrations
Mathilde Collobert / https://mathildecollobert.cargo.site/

Graphisme
Margaux Hallot

La Ligue des Droits Humains est membre de la Fédération internationale pour les droits humains (FIDH), ONG ayant statut consultatif auprès des Nations Unies de l'Unesco, du Conseil de l'Europe et d'observateur auprès de la Commission africaine des droits de l'Homme et des Peuples. La LDH est reconnue en Éducation permanente (FWB) et adhère au code éthique de l'AERF.

Nos soutiens :

FÉDÉRATION WALLONIE-BRUXELLES

Francophones Bruxelles

Emmanuelle de Buisseret Hardy, conseillère juridique à la Ligue des droits humains

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 constituées[4] et l'opacité presque totale qui les entoure[5], 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 population[6]. 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 SudInfo[8] : *« 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 artificielle[10] 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 ces choix politiques – techno-solutionnistes – 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.organedecontrole.be/files/DA210029_Avis_F.pdf, pts 9-10.

10 A 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'État[11] 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.

Sophie Mercier, Boursière FRESH – F.N.R.S.

La Cour constitutionnelle, éternelle funambule ?

Rarement sous le feu des projecteurs, la Cour constitutionnelle est pourtant une juridiction d'une importance capitale. Créée en 1980 sous le nom de « Cour d'arbitrage », elle est aujourd'hui la gardienne du respect des droits fondamentaux et de la répartition des compétences entre les différentes entités (autorité fédérale et entités fédérées). Pour comprendre la manière dont elle réalise le contrôle de conformité des lois, devant être aussi équilibré que possible, nous allons tenter de décrypter son rôle et son fonctionnement dans les lignes qui suivent.

Solide sur ses appuis

Malgré une certaine évolution de son rôle à travers le temps, les compétences principales de la Cour constitutionnelle sont désormais bien balisées : elle doit vérifier « la compatibilité de deux textes, l'un législatif, l'autre constitutionnel, voire la conformité de l'un à l'autre »[1]. Les normes contrôlées sont les normes législatives du niveau fédéral (lois) mais aussi des régions et des communautés (décrets et ordonnances). La Cour s'assure que ces normes respectent certaines règles, les plus importantes, on parle de bloc de constitutionnalité. Il s'agit des règles de répartition de compétence entre les différentes entités, des droits fondamentaux, des règles sur la légalité de l'impôt et du principe de loyauté fédérale[2]. Les droits fondamentaux qui sont protégés sont ceux que l'on retrouve explicitement inscrits dans la Constitution, mais aussi les droits analogues qui sont consacrés dans d'autres textes ratifiés par la Belgique comme la Convention européenne des droits de l'homme ou des règles de droit primaire de l'Union européenne.

Pour réaliser ce travail important, la Cour est composée de douze juges[3]. Est garantie la parité socio-professionnelle (il y a autant d'ancien·nes parlementaires que de juristes) et la parité linguistique (il y a autant de néerlandophones que de francophones). Longtemps exclusivement masculine, il est maintenant prévu que la Cour soit composée « de juges de sexe différent, à raison au moins d'un tiers pour le groupe le moins nombreux, étant entendu que ce groupe doit être représenté dans les deux catégories professionnelles précitées »[4]. Depuis 2019 et la nomination de Yasmine Kherbache, le prescrit légal est respecté et, depuis 2023 et la nomination de Magali Plovie, il y a autant d'hommes que de femmes qui siègent. La nomination des juges de la Cour est hautement politique, puisque, d'après une règle coutumière les candidat·es sont présenté·es par un parti politique, « afin que la composition de la Cour reflète, au moment de cette nomination, le rapport des forces politiques du Parlement au moment de cette nomination »[5]. Un vote à la majorité des deux tiers est ensuite organisé alternativement à la Chambre des représentants ou au Sénat pour confirmer la nomination du ou de la candidat·e proposé·e.

Toujours sur un fil

Si différents textes donnent les bases sur lesquelles reposent les compétences de la Cour, dans les faits, comment procède-t-elle à ce contrôle ? Il faut déjà distinguer deux modes de saisine de la Cour : le recours en annulation et la question préjudicielle.

Le recours en annulation consiste en la demande d'annuler tout ou partie d'une norme législative parce qu'elle violerait une ou plusieurs règles du bloc de constitutionnalité. Pour introduire un tel recours, les requérants (qui peuvent

1 M. Verdussen, « Les missions de la justice constitutionnelle », *Justice constitutionnelle*, 2e édition, Bruxelles, Larcier, 2024, p. 143.
2 Constitution, art. 142.
3 Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, *M.B.*, 7 janvier 1989, art. 31, al. 1er.
4 Voy. le site de la Cour constitutionnelle sur ce point : www.const-court.be/fr/court/presentation/organization (consulté le 24 septembre 2024)
5 G. Rosoux, « Chapitre 3 - Légitimité, indépendance et impartialité du juge constitutionnel » in *Contentieux constitutionnel*, 1e édition, Bruxelles, Larcier, 2021, p. 67.

être des particuliers, des associations, un gouvernement d'une entité fédérée…) doivent justifier d'un intérêt. Si l'acception de l'intérêt est large, en ce compris un intérêt collectif dont peuvent se prévaloir certaines associations, la justification reste néanmoins nécessaire et évaluée par la Cour avant de s'attarder sur le fond. Si donc une loi nous parait discriminatoire (et ainsi violer les articles 10 et 11 de la Constitution), mais que nous ne sommes pas concerné·es par le texte et, dès lors, pas impacté·es, nous ne pouvons pas en demander l'annulation. Par ailleurs, cette demande doit être introduite dans les six mois de sa publication au *Moniteur belge* (la revue où sont rendus publics tous les textes à valeur législative une fois qu'ils ont été votés). On ne peut donc pas demander l'annulation d'une loi à tout moment et indéfiniment.

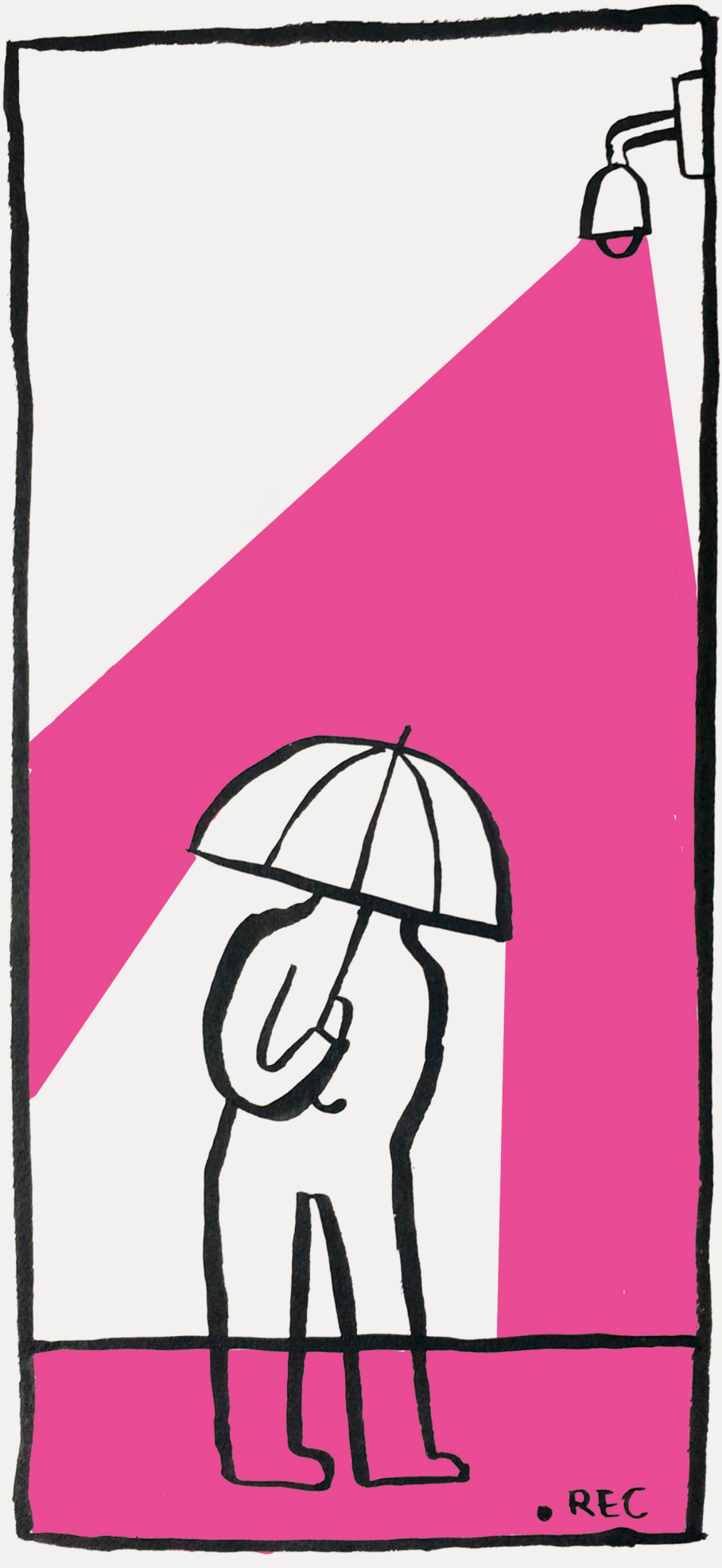
Malgré cela, si le délai pour introduire un recours en annulation est dépassé, il reste une possibilité pour écarter l'application d'une norme inconstitutionnelle. Il s'agit de **la question préjudicielle**. Celle-ci ne peut être posée que par une juridiction dans le cadre d'une résolution de litige, soit de l'initiative de la juridiction elle-même, étant donné qu'une incompatibilité aux normes constitutionnelles est une question d'ordre public, soit à la demande de l'une des parties lors de la procédure[6]. La Cour constitutionnelle est très souple dans la reconnaissance des juridictions qui peuvent s'adresser à elle, il s'agit bien sûr des cours et tribunaux mais aussi de toute autorité saisie d'un recours qui est amenée à se prononcer sur un droit, c'est une application du critère fonctionnel[7]. Il n'y a pas de délai pour poser une question préjudicielle, ce qui permet de supprimer les éventuelles inconstitutionnalités qui n'auraient pas été détectées au départ.

Qu'importe la manière dont elle est saisie, une fois que la requête est considérée comme recevable, la Cour doit agir en véritable équilibriste afin de réaliser un examen fin tenant compte des différents droits et intérêts en balance. Si bien sûr il existe des inconstitutionnalités flagrantes, la plupart du temps la réponse apportée par la Cour suit une structure précise et comporte, généralement, une analyse détaillée de la légalité, de la légitimité et de la proportionnalité de la norme contestée. Elle examine par exemple la clarté des mots choisis, l'application non-rétroactive de certaines dispositions (en matière pénale par exemple), l'adéquation d'une restriction à un droit fondamental…
Lorsque la Cour est saisie d'un recours en annulation et qu'elle constate une violation d'une ou plusieurs règles du bloc de constitutionnalité, elle peut annuler la norme, en tout ou en partie. Cette décision n'est pas susceptible de recours, et donc est définitive et, surtout, elle s'applique à tout le monde. Lorsque la Cour est saisie d'une question préjudicielle et qu'elle constate une violation d'une ou plusieurs règles du bloc de constitutionnalité, l'arrêt est rendu public et communiqué à la juridiction qui avait soulevé la question. C'est cette juridiction qui devra écarter l'application de la norme dans le cadre du litige précis qui l'occupe. La décision de la Cour constitutionnelle ne s'applique donc qu'aux parties du litige[8]. Néanmoins, lorsque la Cour rend un tel arrêt, un nouveau délai de six mois est ouvert pour permettre ainsi l'introduction de recours en annulation.

Parfois sans filet

Dans le funambulisme, pas d'exploit sans prise de risques, et dans le chef de la Cour constitutionnelle, le risque réside dans le fait de chercher sa place dans le système juridique belge et l'exploit de la trouver. En effet, la justice constitutionnelle peut faire l'objet de nombreuses critiques que cela soit par exemple sa légitimité, parce qu'elle sanctionne des actes pris par des assemblées démocratiquement élues, son rapport aux autres institutions, elle peut ne pas être alignée avec les autres juridictions suprêmes ou encore ses interprétations et ses prises de position, on lui reproche tantôt d'avoir été trop loin, tantôt pas assez[9]… Cependant, on s'accorde généralement pour dire que si elle peut être critiquée, la Cour constitutionnelle reste une juridiction absolument essentielle qui peut jouer le rôle de filet de sécurité face à des tendances parfois liberticides des législateurs.

6 M. Verdussen, « Les actes de la justice constitutionnelle », Justice constitutionnelle, 2e édition, Bruxelles, Larcier, 2024, p. 376 et s.
7 C.A., 13 novembre 1996, n°65/96, A.1., M.B., 1997, p. 1431.
8 T. Souverijns et F. Judo, *Prejudiciële vragen praktisch*, 1e édition, Bruxelles, Intersentia, 2017, p. 45.
9 Exemple de doctrine critiquant la position de la Cour : Vrielink, J., Lerouxel, H. et Delgrange, X., « Cachez ce casher que les juges ne veulent voir. À propos de l'arrêt C-336/19 de la Cour de justice de l'Union européenne et des arrêts n°s 117/2021 et 118/2021 de la Cour constitutionnelle relatifs à l'abattage rituel », *A.P.T.*, 2022/4, p. 415-447.


REC

Jérôme Margnys, membre de la commission Nouvelles technologies de la LDH

La vie privée, pour quoi faire ? Exigence démocratique et reconnaissance faciale

Le recours, par l'institution policière, aux technologies de reconnaissance faciale fait aujourd'hui l'objet de vives discussions. Les lignes qui suivent entendent rendre à l'invocation du droit à la vie privée quelque chose de sa charge polémique originale. L'auteur nous invite à concevoir le droit à la vie privée comme un moyen permettant de garantir effectivement la possibilité de résistance ou de désobéissance – ressorts essentiels de l'action politique dans des démocraties nécessairement imparfaites.

Le recours, par l'institution policière, aux technologies de reconnaissance faciale fait aujourd'hui l'objet de vives discussions. **Ses défenseurs mettent généralement en avant** : gains d'efficacité (réduction des taux de criminalités), diminutions des coûts (baisse des effectifs policiers) ou amélioration des conditions de travail (dispensant les policiers de fastidieuses enquêtes). **Ses détracteurs leur opposent** : une relative inefficacité (donnant lieu à des erreurs importantes de discrimination), une augmentation des coûts (licences logicielles, caméras haute définition et puissants serveurs) ainsi que des risques pour certains droits humains, notamment : le droit à la vie privée – tel qu'il se trouve consacré par l'article 8 de la convention européenne des droits de l'homme. Dans les lignes qui suivent, je m'attacherai à compliquer cette invocation du droit à la vie privée, souvent vague et dogmatique, afin de lui restituer quelque chose de sa radicalité politique originale. L'enjeu est au moins double. Contre l'invocation vague : esquisser quelques-uns des effets concrets de la reconnaissance faciale sur des situations sociales. Et contre l'invocation dogmatique : avancer des *raisons* de penser le droit à la vie privée comme un bien devant être préservé, plutôt que comme une contrainte devant être levée.[1]

Précisons les termes. Les systèmes de reconnaissance faciale, auxquels nous nous intéresserons dans les pages qui suivent, articulent typiquement : (i) une base de données rassemblant des images de personnes, (ii) une base de données centralisant des flux de vidéo-surveillance, (iii) des algorithmes permettant de croiser, à des fins d'identification, les images contenues dans ces deux bases de données. En théorie, la police belge peut recourir aux technologies de reconnaissance faciale si et seulement si une disposition légale l'autorise explicitement à consulter des bases de données rassemblant des images de personnes à des fins de reconnaissance faciale. La seule base de données remplissant aujourd'hui ces conditions est une base de données européenne visant à faciliter les contrôles d'identité des demandeurs d'asile par les policiers. En pratique, des enquêtes administratives, journalistiques et académiques ont permis d'établir que la police belge – aux niveaux local comme fédéral – a effectivement recouru, ces dernières années, à plusieurs reprises, à des systèmes de reconnaissance faciale, en dehors de tout cadre légal. Les avancées en analyse automatique d'image, le recours de plus en plus fréquent par la police à la reconnaissance faciale et la relative pauvreté des arguments avancés dans les discussions parlementaires nous imposent de réfléchir à ces enjeux politiques.[2]

1 Les lignes qui suivent ne s'attardent donc pas sur les critiques visant son inefficacité ou son coût, dans la mesure où celles-ci ne concernent que peu la reconnaissance faciale : elles n'auraient pas grand chose à dire de systèmes ne faisant que peu d'erreurs ou ne représentant qu'un coût modeste.

2 Pour les rapports de l'Organe de l'Information Policière, voir : DIO19005 et DIO21006. Pour un article scientifique établissant l'usage de la reconnaissance faciale par la police belge, voir : Lore Rooseleers and Jeroen Maesschalk, 'Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we?' Panopticon. Vol. 42, no. 5, 2021 p. 419-438. Pour un article de presse discutant du recours à la recon-

La reconnaissance faciale nous met d'abord face à un problème posé par la plupart des dispositifs répressifs. Ceux-ci cherchent généralement à accroître l'asymétrie de pouvoir entre gouvernants et gouvernés --- schématiquement : *un* policier armé d'un fusil automatique peut plus facilement contraindre *plusieurs* individus. Le problème posé par ces dispositifs tient alors à la tension, à laquelle semble confrontée la plupart des institutions politiques, entre exigences sécuritaire et démocratique. L'exigence sécuritaire pose la nécessité de la préservation des biens et des personnes. Elle se matérialise aujourd'hui, le plus souvent, par l'engagement d'effectifs policiers et l'acquisition de dispositifs techniques. Elle contribue, de fait, à creuser l'asymétrie entre gouvernants et gouverné·es – sans laquelle la sécurité ne pourrait être garantie. L'exigence démocratique pose, idéalement au moins, l'identité des gouvernants et des gouvernés. Les décisions démocratiques seraient ainsi respectées, non pas tant en raison de l›effectivité d'un appareil répressif, qu'en raison de leur capacité à répondre de façon exigeante aux problèmes vécus par l'ensemble des personnes concernées. L'exigence démocratique semble, de fait, associée à une relative symétrie entre gouvernants et gouvernés – sans laquelle la démocratie finirait par emprunter à la tyrannie ses moyens. La difficulté propre au raisonnement politique tient à la nécessité d'articuler ces deux exigences : démocratique et sécuritaire.

La reconnaissance faciale nous met ensuite face à un problème posé par la plupart des dispositifs techniques. L'enjeu est ici de saisir l'ensemble des transformations sociales susceptibles d'être suscitées par de tels dispositifs. Nous sommes souvent amenés à porter notre attention sur ces quelques tâches, habituellement exercées par les humains, que les ingénieurs semblent effectivement parvenir à déléguer à des dispositifs techniques – dans notre cas : une tâche relativement limitée de comparaisons d'images. Le risque tient à ce que nous négligions une série d'autres transformations, notamment : l'écart entre les tâches effectuées par les humains et les tâches déléguées aux machines. Dans le cas des systèmes de reconnaissance faciale, cette transformation est au moins double. En premier lieu : l'automatisation permet de charger *un* système informatique de ce qu'autrement une *multitude* d'humains devraient faire. Elle limite le nombre d'humains nécessaires à l'exécution d'une telle tâche. En second lieu : l'automatisation stabilise l'exécution d'une directive qui aurait pu trouver, dans certains contextes, à ne pas être appliquée ou à être appliquée différemment. Les technologies de reconnaissance faciale ont donc bien pour caractéristiques essentielles d'accroître l'asymétrie entre gouvernants et gouverné·es et de limiter les opportunités de désobéissance.

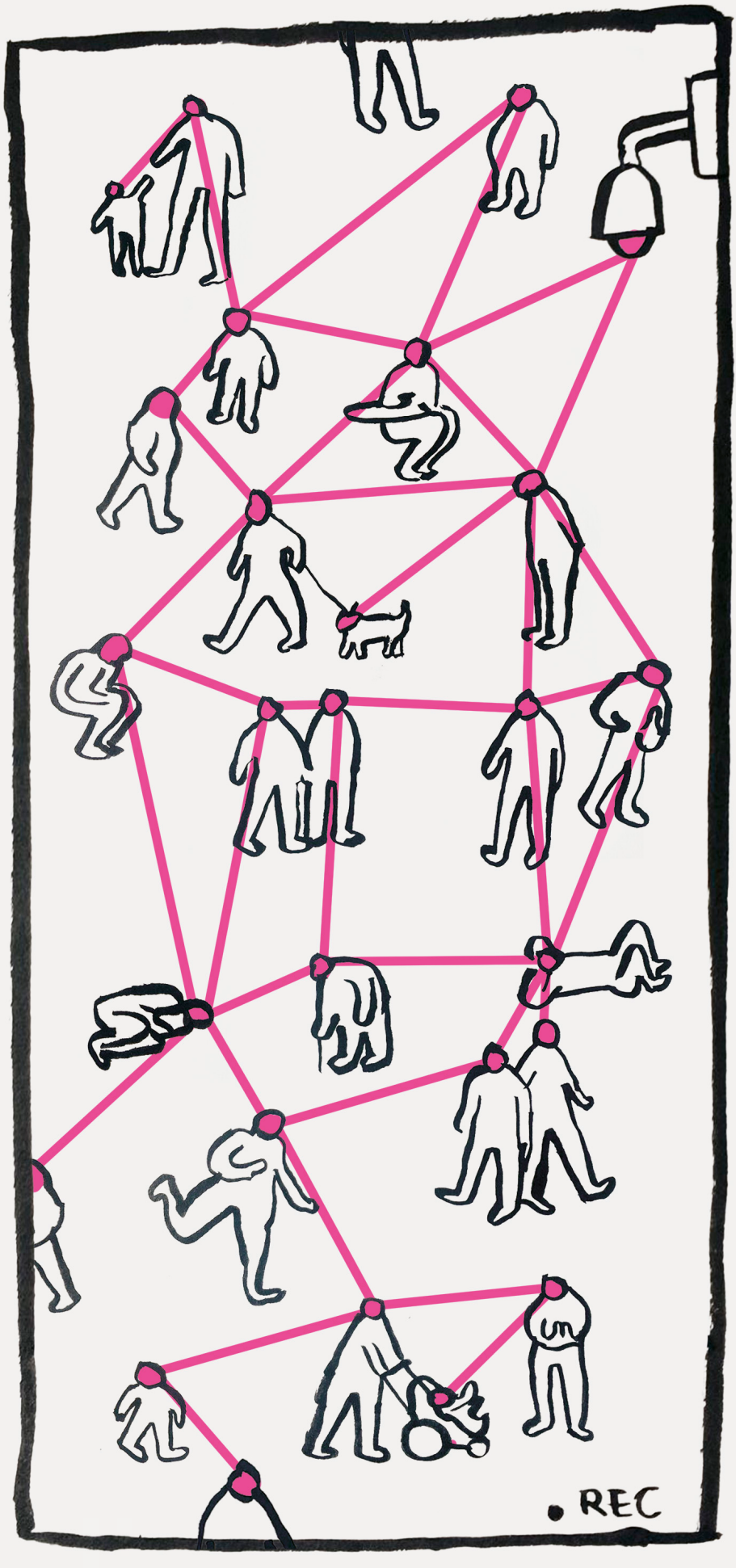
Le problème se ramène alors à la question de savoir s'il est politiquement intéressant de construire des espaces communs au sein desquels la résistance aux institutions devient pratiquement impossible. La difficulté tient dès lors à ce qu'il nous faut apprécier les rôles que peuvent jouer les mouvements de désobéissance ou de résistance – légaux ou illégaux, civils ou incivils – dans l'acquisition d'avancées sociales, morales et politiques. Historiquement, le mouvement américain des droits civiques, militant pour l'abolition des dispositions légales organisant la ségrégation raciale, illustre de façon particulièrement claire l'importance pratique de la possibilité de désobéir et de résister, afin de voir certaines luttes progresser. Politiquement, la résistance est souvent considérée comme légitime dès lors que les voies traditionnelles ne permettent pas aux institutions démocratiques d'entendre ou de prendre en charge certains des problèmes les plus criants et urgents vécus par leurs citoyen·nes. Dit autrement : il revient aux défenseurs de la reconnaissance faciale de montrer que celle-ci ne menace pas de priver les citoyens de stratégies pourtant essentielles à nos vies démocratiques.

naissance faciale par la police belge, voir : Françoise de Halleux, « Comme au procès Pélicot, la police belge utilise aussi un logiciel de reconnaissance faciale », sudinfo.be, 10/09/2024.

> *"Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Ce droit englobe le droit à un nom, le droit au changement d'état civil et à une nouvelle identité, la protection contre les écoutes téléphoniques, la collecte d'informations à caractère privé par les services de sécurité d'un Etat et les publications portant atteinte à la vie privée. Ce droit permet aussi aux membres d'une minorité nationale d'avoir un mode de vie traditionnel".*[3]

Le droit à la vie privée m'intéresse ici surtout dans la mesure où il semble contribuer à la préservation, même minimale, des possibilités de désobéissance et de résistance vis-à-vis de nos institutions démocratiques. L'argument – s'il fait du droit à la vie privée un *moyen* plutôt qu'une *fin* – présente deux avantages, au moins. D'abord, il part de présupposés qui me semblent largement partagés, principalement : l'importance et la faillibilité des institutions démocratiques quant à l'organisation de la vie en commun. Ensuite, il contribue à renverser la charge de la preuve : il revient maintenant aux défenseurs de ces technologies de montrer que celles-ci ne mettent pas en péril certains des ressorts essentiels aux processus démocratiques. Pour autant, l'argument ne permet pas de conclure à la nécessité d'interdire la reconnaissance faciale : il nous invite d'abord et surtout à faire droit aux exigences sécuritaire et démocratique. Il est possible de reformuler ce qui vient d'être dit, de façon plus provocante. L'exigence sécuritaire ne serait en réalité pas assez ambitieuse : se concentrant exclusivement sur les gouverné·es, elle manque de voir que l'insécurité est parfois le fait des gouvernants.

3 Article 8 de la Convention européenne des droits de l'homme.


• REC

Jean-Michel Decroly, professeur de géographie, démographie et tourisme à l'Université Libre de Bruxelles

Les Jeux olympiques de Paris 2024 : cheval de Troie de la vidéosurveillance algorithmique

A plusieurs titres, les éditions récentes des Jeux olympiques ressemblent aux guerres : elles sont l'occasion de la mise en place d'un régime d'exception, donnent lieu au déploiement d'imposants dispositifs de sécurité et constituent un terreau fertile pour tester et normaliser de nouvelles technologies, notamment dans le domaine de la surveillance des populations[1]. Les Jeux de Paris 2024 n'ont pas dérogé à cette tendance lourde, puisque les mesures de sécurité y ont été exceptionnelles et qu'ils furent le théâtre d'une expérimentation d'une version « augmentée » de la vidéosurveillance.

Régime d'exception

Depuis plusieurs olympiades, l'organisation d'une édition des Jeux conduit à la mise en place d'un régime d'exception[2]. Un régime qui fait penser au capitalisme du désastre, le concept formulé par Naomi Klein[3]. C'est d'ailleurs par analogie avec ce dernier que Jules Boykoff a forgé le concept de capitalisme de fête[4]. A ces yeux, les Jeux olympiques se déroulent dans un état d'exception, qui n'est pas provoqué par une catastrophe environnementale, une crise sanitaire ou une guerre, comme dans le capitalisme du désastre, mais bien par le gigantisme et l'exubérance d'une grande manifestation sportive. Dans les deux cas, toutefois, la situation exceptionnelle permet de court-circuiter le processus démocratique : les règles normales de la politique sont temporairement suspendues.

Concrètement, le régime d'exception mis en place à l'occasion d'une édition des Jeux olympiques se traduit par l'adoption de législations qui facilitent l›expropriation, allègent les dispositifs d'évaluation des projets, accélèrent l'approbation des projets d'aménagement, réduisent certains droits des travailleurs et autorisent la mise en œuvre de mesures exceptionnelles de sécurité et de surveillance[5].

Inflation sécuritaire

Au cours des quatre dernières décennies, les Jeux olympiques ont fait l'objet d'une sécurisation croissante. Celle-ci s'est exprimée principalement par l'extension des périmètres où l'accès et la circulation sont interdits ou limités, et le renforcement des mesures de surveillance dans et autour de ces périmètres. Sur le plan des mesures de surveillance, les Jeux d'Athènes en 2004 - les premiers à s'être tenus après les attentats du 11

1 Le contenu de cet article repose en grande partie sur le contenu d'une des sections de l'ouvrage que j'ai récemment consacré aux effets socio-environnementaux des Jeux olympiques (Decroly, J.-M. (2024). Les Jeux olympiques en valent-ils la chandelle ? Bruxelles : Editions de l'Université de Bruxelles.

2 Wolfe, S. D., Gogishvili, D., Chappelet, J. L., & Müller, M. (2022). The urban and economic impacts of mega-events: mechanisms of change in global games. *Sport in Society*, 25 (10), 2079-2087.

3 Klein, N. (2008). *La Stratégie du choc : la montée d'un capitalisme du désastre*. Arles : Actes Sud

4 Boykoff, J. (2013). *Celebration capitalism and the Olympic Games*. Abingdon : Routledge.

5 Voir par exemple : Coaffee, J. (2015). The uneven geographies of the Olympic carceral: from exceptionalism to normalisation. *The Geographical Journal*, 181 (3), 199-211 et Müller, M., & Gaffney, C. (2018). Comparing the urban impacts of the FIFA World Cup and Olympic Games from 2010 to 2016. *Journal of Sport and Social Issues*, 42 (4), 247-269.

septembre 2001 - ont marqué une rupture. Pour mettre en place un « super-panopticon », les autorités grecques ont dépensé plus de cinq fois le budget de sécurité de Sydney 2000[6]. Ils déployèrent plus de 70 000 policiers et soldats spécialement formés sur les sites olympiques, alors que 35 000 autres militaires patrouillaient dans les rues. L'armée et la police eurent aussi largement recours à de multiples dispositifs de sécurité, par exemple 13 000 caméras de surveillance. Le processus de militarisation des Jeux s'est ensuite amplifié, notamment lors de Londres 2012 : des missiles sol-air ont été placés à divers endroits de Londres, l'espace aérien de la ville a été quadrillé par des avions et des hélicoptères de combat et des tireurs d'élites étaient déployés dans la ville avec l'autorisation d'utiliser leurs armes[7]. Ces déploiements spectaculaires de membres de forces de l'ordre, d'armes et de dispositifs de surveillance font que les Jeux olympiques donnent lieu, à l'heure actuelle, aux plus grandes opérations à caractère sécuritaire en-dehors des guerres[8].

INNOVATIONS PARISIENNES

Les Jeux olympiques de Paris 2024 ont à nouveau donné lieu à un impressionnant déploiement sécuritaire. Les services de police ont établi plusieurs périmètres de sécurité autour des sites de compétition, au sein desquels la circulation était très fortement limitée, voire interdite pour les zones proches des enceintes sportives. Par ailleurs, jusqu'à 45 000 policiers et gendarmes français ont été mobilisés pour assurer la surveillance de l'événement dans la seule agglomération parisienne, auxquels se sont ajoutés près de 2000 policiers internationaux, 21 000 agents de sécurité privée et au moins une dizaine de milliers de militaires de l'opération Sentinelle[9]. Au total, ce sont près de 80 000 membres des forces de l'ordre publiques et privées qui ont surveillé le déroulement des Jeux olympiques, soit environ 1 membre pour 7 spectateurs présent en moyenne par jour.

Paris 2024 a aussi donné lieu, de manière plus discrète et moins médiatisée, à une expérimentation grandeur nature de la vidéosurveillance algorithmique ou automatisée (VSA). En effet, la loi « olympique » adoptée par le parlement français en avril 2023 a autorisé à titre expérimental, mais jusque fin mars 2025, « le traitement algorithmique d'images collectées par des systèmes de vidéoprotection ou par des caméras installées sur des aéronefs (notamment des drones) ». La loi précise qu'au terme des Jeux olympiques, l'expérimentation concernera uniquement des événements (sportifs, culturels ou récréatifs) de grande ampleur donc considérés comme étant exposés à des risques, notamment terroristes. L'objectif est que ce nouveau dispositif facilite, dans et aux abords des lieux accueillant du public et des réseaux de transport, la détection des situations jugées à risques.

Sur le plan technique, la VSA est une nouvelle venue dans les instruments de surveillance de la population. Pour faire simple, il s'agit d'un système de vidéosurveillance qui a recours à l'intelligence artificielle. Sur le plan pratique, il consiste à automatiser le traitement d'images de caméras de surveillance en mobilisant des algorithmes qui permettent une analyse automatique, en temps réel et en continu, des images captées et la transmission, toujours automatique, d'un signalement à destination de la police en cas de détection d'un événement jugé suspect en fonction de critères préalablement établis. Dans le cadre de la loi d'avril 2023, huit types d'événements considérés comme « anormaux » peuvent faire

6 Samatas, M. (2011). Surveillance in Athens 2004 and Beijing 2008: A comparison of the Olympic surveillance modalities and legacies in two different Olympic host regimes. *Urban studies*, 48 (15), 3347-3366.
7 Boykoff, J. (2013). *Celebration capitalism and the Olympic Games*. Abingdon : Routledge.
8 Boyle, P. (2012). Securing the Olympic Games : exemplifications of local governance. In : H. J. Lensky & S. Wagg (ed.) The Palgrave handbook of Olympic studies (pp. xxx). London: Palgrave Macmillan..
9 Opération visant à renforcer la sécurité sur le territoire français, qui a été mise en place suite aux attentats du 7, 8 et 9 janvier 2015.

l'objet d'une détection par la VSA : la présence d'objets abandonnés, la présence ou l'utilisation d'armes, le non-respect du sens commun de la circulation par un véhicule ou une personne, la présence d'un véhicule ou d'une personne dans une zone interdite ou jugée sensible, la présence d'une personne au sol suite à une chute, un mouvement de foule, une densité considérée comme trop importante de personnes ou le départ d'incendies.

Des premiers tests de la VSA ont été réalisés au cours du printemps 2024, à l'occasion notamment de concerts donnés à l'Accor Arena (ex-Paris-Bercy). Lors des Jeux eux-mêmes, suite à des autorisations octroyées par le préfet de police de Paris, ce ne sont pas moins de 485 caméras dont les images ont fait l'objet d'une analyse par un logiciel d'intelligence artificielle. Ces caméras faisaient partie du réseau de vidéosurveillance de la RATP, de la SNCF ou de la préfecture de police de Paris. Elles étaient disposées dans des stations de métro, des gares ou sur la voie publique à proximité des enceintes sportives où se déroulaient les compétions.

EXTENSION DU DOMAINE DE LA SURVEILLANCE ET FLOU JURIDIQUE

A l'exception des associations qui luttent contre l'extension de la surveillance de l'espace publique et de certains journalistes ou intellectuels critiques, l'utilisation de la VSA lors des Jeux de Paris n'a pas suscité de vives réactions. Il est vrai que, conformément aux règles en vigueur au sein de l'Union européenne, elle ne pouvait en aucune manière donner lieu à des formes de reconnaissance faciale. Pourtant, le passage à la VSA marque un tournant dans la surveillance de l'espace public par les services de l'État. En effet, avec ces nouvelles technologies, ils disposent dorénavant d'un outil permettant un contrôle constant et automatisé de ce qui s'y passe. De plus, la VSA conduit à une discrimination des individus en fonction de leur manière d'agir dans l'espace public. Enfin, les contours de la plupart des conduites jugées « anormales » ne sont pas publicisés. Le·a citoyen·ne en est réduit·e à se demander ce qu'est une zone considérée comme « sensible », à partir de quand les flux de personnes dans l'espace public deviennent un « mouvement de foule » et sur base de quels critères la densité de personnes est-elle jugée « excessive ».

Bien qu'encadré par la loi d'avril 2023, la mise en œuvre du dispositif se caractérise aussi par son flou juridique et son manque de transparence. Les arrêtés d'autorisation de l'utilisation de la VSA ont été publiés très tardivement, ce qui a rendu impossible le dépôt d'éventuels recours. Alors que la législation établissait une liste restrictive d'acteurs publics autorisés à recourir à la VSA, la préfecture de police a néanmoins autorisé son déploiement à Paris Expo Porte de Versailles, en utilisant des caméras de Viparis, le gestionnaire du site, qui ne figurait pas dans ladite liste. De surcroît, dans les lieux de déploiement des caméras « augmentées », les personnes susceptibles d'être filmées n'ont pas été correctement informées de la nouvelle forme de surveillance dont elles faisaient l'objet.

ELARGISSEMENT DU MARCHÉ DE LA SURVEILLANCE ET FANTASME DE LA POLICE PRÉDICTIVE

L'expérimentation de la VSA lors de Paris 2024 a permis aux firmes les mieux insérées sur le marché de la vidéosurveillance de pouvoir se positionner sur un nouveau créneau porteur. A court terme, elle a conduit au lancement par le ministère français de l'Intérieur d'un appel d'offre qui a débouché sur l'octroi d'un budget d'environ 8 millions d'euros publics à quatre firmes françaises. A plus long terme, elle devrait faciliter l'obtention des futurs et juteux contrats par des entreprises soucieuses de ne pas être débordées par les géants chinois et étasuniens du secteur. Le développement de ce marché ne manque pourtant pas d'étonner. En effet, sur le plan technique la VSA a davantage fait ses preuves sur le papier glacé des brochures de ses promoteurs que sur le terrain. Depuis une

dizaine d'années, en-dehors des tests réalisés pour repérer les départs d'incendies, la plupart des expériences de vidéosurveillance intelligente ont donné lieu à des échecs cinglants, avec une proportion souvent élevée de « faux positifs » (personnes qui sont identifiées comme suspectes par le logiciel mais qui sont de fait innocentes). Ces échecs à répétition n'ont toutefois pas refroidi les ardeurs de nombreuses collectivités territoriales, qui continuent à être fascinées par les promesses d'une détection automatique des comportements suspects dans l'espace public.

Vers une normalisation de la VSA

La mise en œuvre de la VSA dans le cadre des Jeux de Paris prépare le déploiement futur de cette technologie de surveillance et un élargissement progressif de ses usages[10]. A cet égard, les propos tenus par le préfet de police de Paris lors d'une audition devant la commission des lois de l'Assemblée nationale à la fin septembre 2024 sont édifiants. Il a effet défendu que la VSA avait montré son « utilité » lors des Jeux et qu'il convenait de prolonger son utilisation au-delà du mois de mars 2025. En s'exprimant de la sorte, le préfet de police illustre la banalisation en matière de sécurité et de surveillance du principe qui consiste à imposer comme nouvelle norme des dispositifs utilisés à titre exceptionnel, en particulier à la suite d'attentats ou lors de grands événements. La VSA est donc en train d'entrer dans le droit commun. Et elle le fera d'autant plus facilement qu'elle est associée à un souvenir d'euphorie collective, dont l'existence même en aurait soi-disant dépendu. La réussite de l'organisation des Jeux olympiques parisiens va donc servir à consolider l'acceptabilité sociale d'un contrôle accru des citoyen·nes dans l'espace public. Ce n'est pas le moindre des paradoxes pour un événement qui a célébré avec faste les libertés individuelles lors de sa cérémonie d'ouverture.

10 La Quadrature du Net (2024). VSA et Jeux olympiques : coup d'envoi pour les entreprises de surveillance. https://www.laquadrature.net/2024/01/26/vsa-et-jeux-olympiques-coup-denvoi-pour-les-entreprises-de-surveillance/

Chloé Berthélémy, Conseillère politique, European Digital Rights (EDRi)

Mais que fait l'Europe ?

La reconnaissance faciale se déploie à travers tout le continent. Souvent dans l'opacité, sans débat public. Parfois même de manière illégale. En réponse l'Union européenne (UE) a adopté en 2024 l'acte sur l'intelligence artificielle. Il vise à encadrer ces nouvelles technologies qui risquent de nous faire basculer dans une société de surveillance de masse. Malheureusement, au terme de nombreux compromis politiques, la loi échoue largement à enrayer la prolifération de ces technologies liberticides.

ÇA PARTAIT MAL : QUAND L'APPROCHE ÉCONOMIQUE DOMINE

En avril 2021, la Commission européenne révèle sa proposition législative pour un acte européen sur l'intelligence artificielle (AIA). Les mesures de protection des droits fondamentaux y sont modestes, largement inefficaces face aux risques présents et futurs que posent ces systèmes technologiques. Pas de surprise néanmoins, car la nature des débats précédents la publication annonçaient déjà la couleur.[1] L'objectif politique affiché et assumé est de réguler *a minima* le marché de l'intelligence artificielle (IA) en plein essor. Le mode d'ordre, c'est l'innovation.
Empêtrée dans un discours qui place l'UE dans une course technologique effrénée contre les États-Unis et la Chine et devant déjà « rattraper notre retard », la Commission favorise une régulation légère de l'IA. C'est un marché qu'il ne faudrait pas accabler par un trop-plein d'obligations juridiques contraignantes et coûteuses à respecter. Les start-ups européennes doivent pouvoir innover librement, devenir compétitives sur le marché mondial, et ainsi, contribuer à « *la souveraineté numérique européenne* ». On verra plus tard pour les coûts sociétaux, politiques et environnementaux.

Le texte donne par conséquent une grande place à l'auto-régulation et choisit une approche basée sur les risques posés par les systèmes d'IA. Quatre niveaux de risque (négligeable, limité, élevé et inacceptable) sont établis plus ou moins explicitement pour classer les types d'IA ou leur champ d'application (éducation, emploi, police, etc.). Les développeurs eux-mêmes sont chargés d'évaluer dans quelle catégorie tombent leurs systèmes. Ce seront donc les entreprises, avant tout motivées par le profit, qui déterminent quelles exigences elles doivent ou non respecter. Et il leur appartiendra aussi de juger si elles ont suffisamment satisfait à ces exigences fixées en matière de traitement des données, d'exactitude, de transparence, etc. Les mécanismes de supervision, qui par défaut interviennent a posteriori de la mise sur le marché et l'utilisation de l'IA, échoueront à systématiquement détecter les abus, les erreurs et les défauts de conformité et donc à prévenir les dommages.

En outre, les obligations ne sont vraiment pas strictes. Pour les IA à risques limités, un peu de transparence vis-à-vis des personnes qui interagissent avec elles. Pour les systèmes à hauts risques, il s'agit principalement de se mettre en conformité avec des standards techniques, définis par des organismes de standardisation de droit privé. Ces règles sont le fer de lance de la proposition de la Commission européenne et pourtant selon sa propre évaluation, elles ne toucheraient que de 5 à 15 % des systèmes d'IA mis sur le marché de l'UE.

Là s'illustrent toutes les lacunes de la loi. D'abord son approche purement économique qui traite l'IA comme un simple produit industriel passe sous silence un grand nombre de risques. Pensons notamment au renforcement des inégalités structurelles, des rapports de pouvoir, des

1 https://la-rem.eu/2024/03/loi-europeenne-sur-lia-une-reglementation-digne-de-con%ef%ac%81ance/

impacts environnementaux, des formes nouvelles d'exploitation sur le marché du travail, ou encore de l'extractivisme dans les pays du Sud Global. Sans parler de la dépendance croissante vis-à-vis des entreprises de la tech et la plus grande acceptation sociale de la surveillance de masse. Deuxièmement, elle ne tient pas compte de la complexité des systèmes d'IA et de l'importance du contexte pour pouvoir évaluer leurs impacts sur les droits fondamentaux et sur la société plus globalement. En se concentrant sur les critères à remplir du fournisseur de l'IA, et non des utilisateurs, le mécanisme est fondamentalement mal adapté pour identifier les risques dans le contexte du déploiement. Par exemple, un système de reconnaissance faciale déployé dans un centre commercial peut satisfaire aux exigences techniques spécifiées dans la loi, tout en constituant une violation importante des droits fondamentaux en compromettant la protection des données, violant la vie privée ou l'interdiction de discriminer.

L'ACTE SUR L'IA ET LA SURVEILLANCE BIOMÉTRIQUE : PROTECTEUR OU PERMISSIF ?

Au cours des négociations entre le Parlement européen et le Conseil des États-Membres, quelques règles ont tout de même été introduites pour pallier cette zone de quasi-non-droit pour les utilisateurs d'IA à hauts risques. Dans le texte final, on trouve donc des obligations en matière d'accessibilité (en particulier pour les personnes en situation de handicap) et de transparence (inscription dans un registre européen des buts de l'usage de l'IA et de sa logique de fonctionnement). De plus, les déployeurs devront mener une étude d'impact sur les droits fondamentaux et en publier un résumé. Les personnes affectées par les systèmes d›IA, quant à elles, obtiennent quelques voies de recours, bien que certainement peu efficaces dans la pratique.

Ces mesures supplémentaires sont très loin d'être suffisantes et sont truffées d'exceptions. La transparence, oui, mais que pour les autorités publiques car le « secret des affaires » doit être préservé avant tout. Il n'y a pas de comptes à rendre non plus dans les domaines migratoire et de contrôle des frontières. L'UE poursuit son régime d'exceptionnalisme envers les migrant·es et demandeur·ses d'asile, qui se retrouvent à nouveau avec moins de protection que le reste de la population. Enfin, la police, elle aussi, est exemptée de tout devoir de transparence envers le public et peut même déployer une IA à haut risque avant d'en avoir obtenu l'autorisation au nom de la « sécurité publique ».

Mais qu'en est-il des IA présentant des risques inacceptables ? Si demain la police belge veut déployer de la reconnaissance faciale dans les rues, que dit le règlement ? Malgré sa liste de systèmes d'IA interdits, le cadre légal européen reste globalement permissif vis-à-vis de toute une série d'usages, dont les effets néfastes sont pourtant bien connus et documentés. À nouveau, à peine a-t-on établi une règle, qu'on en restreint immédiatement la portée en créant de multiples exceptions.

Le recours à « l'identification biométrique à distance en temps réel », telle que la reconnaissance faciale déployée sur les passant·es d'un centre-ville pour repérer celleux qui figurent une liste de surveillance, n'est interdit que pour la police dans les espaces accessibles au public.[2]

Toutefois elle pourra l'utiliser dès lors qu'il s'agit de retrouver des personnes disparues ou des victimes d'enlèvement ou de la traite sexuelle, en cas de « menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques », ou encore pour prévenir une menace terroriste.

2 https://www.laquadrature.net/2024/01/19/le-reglement-europeen-sur-lia-ninterdira-pas-la-surveillance-biometrique-de-masse/

Non seulement ces motifs peuvent être facilement abusés et leur définition élargie, comme c'est déjà le cas des politiques antiterroristes en Europe qui mènent systématiquement à la sur-répression des communautés musulmanes, mais la liste peut rapidement s'allonger dans le futur.

Pourtant les expérimentations montrent déjà tous les effets dystopiques de ces systèmes. En plus de faire des erreurs souvent lourdes de conséquences (surtout pour les personnes racisées[3]) en dépit de taux d'exactitude élevés affichés[4], ils décuplent le pouvoir étatique de surveillance. Les personnes qui tentaient d'éviter de passer devant les caméras de Londres, ou qui exerçaient leur droit légitime de leur résister en se couvrant le visage, ont été arrêtées et, dans certains cas, condamnées à une amende.[5]

Pire encore, au lieu de tracer des lignes rouges face aux risques sociétaux en jeu, l'AIA ouvre potentiellement la voie à la légalisation de certaines utilisations de ces systèmes pour la première fois dans l'UE. Les exceptions en série donnent le signal que certaines formes de surveillance biométrique de masse ou de discrimination alimentée par l'IA sont légitimes dans certaines circonstances.

C'est le cas des systèmes de reconnaissance des émotions – ces IA qui prétendent par exemple pouvoir déterminer sans aucune validation scientifique crédible si quelqu'un·e ment - qui sont interdits seulement sur les lieux de travail et dans l'enseignement. Sauf pour des « raisons médicales ou de sécurité ». Ils sont aussi permis dans le cadre des missions de police. Une exception en cache une autre.

Il est prohibé d'utiliser des méthodes de catégorisation biométrique (qui peuvent supposément classer les personnes sur la base de leurs caractéristiques physiques) pour déduire la race, les opinions politiques, l'orientation sexuelle, et autres. Mais c'est tout à fait possible pour le genre, le statut de santé, ou la situation de handicap. Et encore une fois, l'interdiction ne concerne pas la police ni les autorités d'immigration. Par conséquent, dans les faits, il sera possible sous droit européen d'autoriser la police à classer les personnes filmées par des caméras de vidéosurveillance en fonction de leur couleur de peau. Cela semble impossible à réconcilier avec la législation européenne en vigueur contre la discrimination.

Ceci témoigne de la volonté de l'UE de laisser les personnes les plus marginalisées de la société devenir les cobayes de tests technologiques les plus intrusifs et déshumanisants.

Malgré quelques outils donnés au combat contre la surveillance biométrique[6], l'AIA est passé à côté d'une grande opportunité de protéger les personnes, les communautés, la société et l'État de droit contre ses dangers. Cette loi met en évidence les fondements idéologiques de l'UE, concentrés sur le marché intérieur et la croissance économique. Elle ne met pas les droits fondamentaux au premier plan, même si c'est ce qu'elle prétend.

3 https://londonnewsonline.co.uk/news/police-facial-recognition-system-has-potential-to-entrench-racial-bias/

4 La police londonnienne a déclaré que leur système était efficace à 70 % pour repérer les suspects recherchés et qu'il identifiait faussement une personne recherchée dans un cas sur mille. Mais le professeur Pete Fussey de l'université d'Essex qui a mené un examen indépendant a constaté que le système n'était exact que dans 19 % des cas. https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras

5 https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

6 https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/#part-1


REC

Rémy Farge, formateur à la LDH

Reconnaissance automatique des émotions, une valeur probante à haut risque

«There is a face beneath this mask, but it's not me.
I'm no more that face than I am the muscles
beneath it, or the bones beneath that.»
V for Vendetta, 2005

Le règlement sur l'intelligence artificielle adopté par l'UE (AI Act) encadre, parfois de façon très permissive, le traitement de données biométriques à des fins d'identification, d'authentification, de catégorisation mais aussi de reconnaissance des émotions. Ces systèmes seraient en mesure d'identifier ou de déduire des émotions ou des intentions sur base de l'analyse du visage, des yeux, de la voix, etc. La police et le contrôle des frontières sont depuis longtemps des domaines d'expérimentation, et ils jouissent dans le règlement d'un traitement dérogatoire propice. Les inquiétudes des spécialistes sont pourtant nombreuses, et les risques largement documentés.

« *Historique* » aux yeux d'Ursula von der Leyen et du commissaire européen Thierry Breton. « *Un pas modeste* » et plutôt « *décevant* » pour EDRi, le réseau européen de défense des libertés en ligne. C'est un enthousiasme très inégal qui s'exprime à l'issue de ce long processus législatif. Au fond, les conclusions qui se dessinent ne font que traduire l'âpreté des débats qui ont animé les négociations, et en premier lieu celles qui concernaient l'utilisation des données biométriques.

Sur la reconnaissance des émotions, l'AI Act reconnaît dans ses considérants que la base scientifique de ces systèmes « suscite de vives inquiétudes, d'autant plus que l'expression des émotions varie considérablement d'une culture et d'une situation à l'autre ». Plusieurs défauts tels que « leur fiabilité limitée, leur manque de précision et leur *généralisabilité limitée* » sont évoqués. Une conséquence possible serait de « conduire à des résultats discriminatoires et [pouvant] être intrusifs pour les droits et libertés des personnes ». Un tel diagnostic suffit-il à expédier cette technologie dans la liste des pratiques inacceptables ? Apparemment pas. L'interdiction de mise sur le marché et d'utilisation de ces systèmes ne vaut que dans les lieux de travail et dans les écoles, sauf si la mise sur le marché se justifie par des raisons médicales ou de sécurité. Outre ces exceptions, l'IA destinée à détecter des émotions est classée à haut risque, donc autorisée sous certaines conditions.

L'IA ÉMOTIONNELLE AU SERVICE DES FORCES DE L'ORDRE ET DU CONTRÔLE DES FRONTIÈRES

Suivant une tendance à l'accumulation et au recours croissant aux données dans toutes les sphères de la société, les promesses en matière de détection des émotions semblent infinies : évaluer la satisfaction d'une clientèle, contrôler la concentration d'une personne au volant, déterminer le score d'employabilité lors d'un entretien, etc. Nul doute que l'AI Act donnera un nouvel élan à ces projets, et notamment ceux développés à destination des services répressifs et des gardes-frontières. Pour ces deux domaines, le Parlement européen prévoyait pourtant une interdiction dans sa position de négociation à l'été 2023, mais c'était sans compter les exigences du Conseil de l'UE et des États-membres.

Des projets de reconnaissance automatique des émotions existent depuis belle lurette, à l'instar d'AVATAR déployé en 2012 à la frontière sud des États-Unis. Ses concepteurs qui collaboraient avec l'université d'Arizona se disaient en mesure de détecter des mensonges en analysant la voix, les yeux et les expressions faciales des répondants souhaitant entrer sur le territoire. En cas de mauvaises réponses (physiologiques), l'interrogatoire suivant était plus approfondi, et face à un humain cette fois. L'Agence britannique de gestion des frontières expérimentait à la même période une machine comparable qui scrutait spécifiquement les expressions du visage et la chaleur corporelle. Plus récemment, un programme européen visant à booster l'innovation et la recherche a permis de financer le projet iBorderCtrl. Afin de déterminer le risque pour la sécurité, l'enregistrement préalable prévoyait des vérifications de plusieurs bases de données, et des informations disponibles publiquement sur les réseaux sociaux de la personne souhaitant voyager. Testé en Hongrie, Grèce et Lettonie jusqu'en 2019, il comprenait aussi l'« Automatic Deception Detection System ». Ce système consistait en l'analyse de micro-expressions faciales afin d'évaluer la véracité des réponses données à un garde-frontière virtuel.

Plusieurs ONG[1] redoutent qu'une fois dans les mains des services de police, la reconnaissance des émotions ne soit utilisée pour prédire des comportements potentiellement « agressifs » lors d'une manifestation. De telles prédictions pourraient entraîner des interventions sans qu'aucun acte infractionnel ne soit effectué. Ces craintes ne paraissent pas infondées. Tandis que certaines entreprises annoncent pouvoir prédire la survenance d'une émeute, la société britannique WeSee dit avoir déjà collaboré avec un service de police dans le cadre d'interrogatoires[2]. L'exemple de la police anglaise de Lincolnshire, sur le littoral Est de l'Angleterre, n'est sans doute pas unique et il illustre une tendance au solutionnisme technologique en matière sécuritaire. En 2020, un fond gouvernemental lui avait permis d'acquérir de nouvelles caméras de vidéosurveillance, des logiciels de reconnaissance faciale, d'analyses des comportements et de reconnaissance de plaque d'immatriculation. Selon la presse, la reconnaissance d'émotions complétait cet arsenal technologique.

From Beijing to Mons, l'essor des pseudosciences

Le marché chinois est sans conteste un des plus gros et les lieux d'expérimentation ne manquent pas. Dans la région du Xinjiang où le contrôle social de la population est poussé à son paroxysme, des systèmes censés détecter des états anxieux ou négatifs ont déjà été testés sur des personnes Ouïghours lors d'interrogatoires. Les résultats serviraient même de *« pré-jugement sans aucune preuve crédible »*[3]. L'influence des entreprises chinoises ne cesse de croître et fait dire à des organisations spécialisées qu'elle risque même d'avoir un impact sur l'élaboration des normes techniques internationales.

Dans tous les cas, les partenariats entre universités et entreprises fleurissent, et jusqu'en Wallonie. L'UMons s'est associée en 2019 avec la start-up MoodMe dans le cadre d'un projet financé par la Région. L'objectif : rendre la reconnaissance faciale et émotionnelle possible sur smartphones. En Wallonie toujours, la start-up néo-louvaniste Piximate propose des produits pour mesurer la satisfaction des consommateurs sur base de l'analyse faciale. La liste de ses clients fut complétée en 2018 par la Gendarmerie française.

À l'image de la reconnaissance faciale, la détection des émotions est utilisée tant à des fins répressives que commerciales. Elle l'est aussi dans le domaine de la médecine. Mais lorsque le secteur de l'IA émotionnelle postule qu'il agit au bénéfice des personnes et de la santé, il ne convainc

1 Access Now, EDRi, Bits of Freedom, Article 19, IT-Pol, Prohibit emotion recognition in the Artificial Intelligence Act, 2023.
2 D. Thomas, The cameras that know if you're happy - or a threat, BBC, 17 juillet 2018.
3 J. Wakefield, AI emotion-detection software tested on Uyghurs, BBC, 26 mai 2021.

pas toujours. En ce qui concerne l'autisme par exemple, le European Council of Autistic People juge que ces technologies sont probablement inutiles pour une proportion significative de personnes autistes et qu'elles témoignent d'une perception erronée de l'autisme. Selon l'organisation, le message normatif en arrière-plan participe souvent à construire une distinction entre expressions émotionnelles 'correctes' et 'pathologiques'. La chercheuse Mara Mills parle même de « prétexte d'assistance » lorsque les concepteurs avancent d'abord un objectif d'assistance pour se tourner par la suite vers des domaines plus rentables. L'investissement du secteur de l'informatique affective dans le champ de la recherche sur l'autisme en serait un exemple[4].

Pendant que la technologie se développe à grand renfort d'aides publiques et que le marché mûrit, bon nombre de scientifiques tentent désespérément de se faire entendre. Le terme de pseudoscience revient souvent pour qualifier les fondements théoriques de cette informatique affective. En 2019, cinq chercheur·ses publièrent une analyse de plus de 1000 articles scientifiques en psychologie et leur conclusion était sans équivoque. Il n'existe pas de preuves suffisantes pour étayer l'hypothèse selon laquelle les êtres humains expriment et reconnaissent de manière fiable certaines émotions dans des configurations spécifiques de mouvements faciaux.[5] Le problème est similaire avec le 'détecteur de mensonges' du projet iBorderCtrl. Le modèle de prédiction se base sur « une chaîne d'hypothèses » qui n'est pas validée scientifiquement[6]. Autrement dit, il établit à tort des relations entre les expressions faciales, les états affectifs, le mensonge et le risque.

UNE PRATIQUE DU POUVOIR AUGMENTÉE

En Belgique, cette technologie pourrait un jour augmenter le pouvoir discrétionnaire de services tels que la police aéroportuaire dont certaines pratiques arbitraires ont déjà valu à l'État belge des condamnations. Dans l'affaire qui concernait l'étudiant congolais Junior Masudi Wasso, les policiers l'avait interrogé, entres autres, sur ses connaissances des transports publics wallons et du chimiste Mendeleïev. Bien que détenteur d'un visa, il avait été transféré en centre fermé. Si ces policiers avaient été équipés d'un détecteur de stress ou de mensonge, les interprétations du logiciel n'auraient probablement pas été à son avantage. Elles auraient même pu participer à la décision discriminatoire de l'Office des étrangers de le placer en détention.

Si la précision et la base scientifique pêchent, aux yeux de beaucoup, la nature même de ces dispositifs sociotechniques doit être interrogée au regard du mode de gouvernance dans lequel ils s'inscrivent. La question de l'exactitude des résultats de la technologie laisse alors place à celle de la pratique du pouvoir qu'elle permet. Utilisés pour détecter la tromperie ou l'anxiété, elle semble effectivement coïncider avec le projet politique, voire idéologique, qui sous-tend le renforcement des frontières et la diminution des possibilités d'accès au territoire. Ce mouvement d'intensification de la répression à l'intérieur et à l'extérieur des frontières s'accompagne du déploiement des technologies idoines pour la mettre en œuvre : caméras thermiques et infrarouges, fichage biométrique, reconnaissance faciale, détection automatisée de mensonges et d'émotions, etc. Dès lors, le choix du législateur européen de faire des activités répressives et de la gestion des frontières un domaine souvent dérogatoire[7] parait cohérent, sinon révélateur. Le règlement est maintenant adopté. La voie est libre pour l'IA émotionnelle et sera semée d'embûches pour qui voudra lui faire face.

4 E. Kang, On the Praxes and Politics of AI Speech Emotion Recognition, Proceedings of the ACM Conference on Fairness, Accountability, and Transparency, 2023, p.462.
5 L. F. Barrett, R. Adolphs, S. Marsella, A. M. Martinez, S. D. Pollak, Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. Psychological Science in the Public Interest, 20, 2019.
6 J. Sánchez-Monedero, L. Dencik, The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl, Information, Communication & Society, 2020.
7 C. Crichton. Règlement sur l'intelligence artificielle. Premiers éléments d'analyse. 2024.

La Ligue dans votre quotidien

Vous souhaitez vous investir dans une section locale de la Ligue des droits humains ? La LDH est aussi près de chez vous !
Vous souhaitez mettre sur pied une section locale LDH ou une/des activités visant à soutenir notre association :
Contactez le secrétariat de la LDH au 02/209 62 80 – ldh@liguedh.be

La Louvière	Marie-Louise ORUBA	064/22 85 34	marielou.oruba@hotmail.com
Liège	Adrien DE RUDDER		liege@liguedh.be
Namur	Christophe DE MOS	0472/66 95 45	namur@liguedh.be
Verviers	Jeannine CHAINEUX	0474/75 06 74	jeannine.chaineux@skynet.be

LA LDH SUR LE WEB

liguedhbe
liguedh_be
LDH BELGIQUE
ligue_des_droits_humains

Aidez-nous à défendre vos droits fondamentaux !

La Ligue des droits humains est une association indépendante. Elle ne peut survivre sans l'apport financier des citoyen·nes qui souhaitent qu'elle continue son combat au quotidien pour la défense des droits fondamentaux en Belgique. Vous pouvez nous soutenir concrètement.

- A partir de 65€ (52,50€ étudiant·e·s, sans emploi, pensionné·e·s), vous devenez **membre donateur·rice.** Vous recevez une déduction fiscale.

- A partir de 25€ (12,5€ étudiant·e·s, sans emploi, pensionné·e·s), vous devenez **membre.** Vous profitez des avantages exclusifs réservés aux membres.

- A partir de 40€, vous devenez **donateur·rice** et profitez d'une déduction fiscale.

La LDH adhère au Code éthique de l'AERF. Vous avez un droit à l'information. Ceci implique que les donateurs, collaborateurs et employés sont informés au moins annuellement de l'utilisation des fonds récoltés. Le rapport d'activités et le bilan financier de la LDH sont consultables sur www.liguedh.be

Ligue des droits humains asbl · Boulevard Léopold II 53 à 1080 Bruxelles
Tél. : 02 209 62 80 · ldh@liguedh.be · www.liguedh.be

Vous aussi, rejoignez-nous !

❑ Je souhaite devenir **membre donateur·rice** et je verse …….. (à partir de 65€/52,50€)
❑ Je souhaite devenir **membre** et je verse …….. (à partir de 25€/12.5€)
❑ Je souhaite devenir **donateur·rice** et je verse …….. (déductible à partir de 40€)

sur le compte de la Ligue des droits humains : IBAN BE89 0000 0001 82 85 - BIC BPOTBEB1

Facilitez-vous la vie : versez via un ordre permanent (OP) !
Pour ce faire, divisez votre montant par 12 et contactez votre organisme bancaire pour la procédure.

❑ Je verse le montant via un ordre permanent
❑ Vous pouvez également vous rendre sur **www.liguedh.be** et effectuer un paiement en ligne à l'aide de votre carte de crédit

PayPal

Nom : Prénom :
Adresse :
Année de naissance : Profession :
Tél : Courriel :
Signature :