La Chronique
de la Ligue des droits humains asbl
n°203

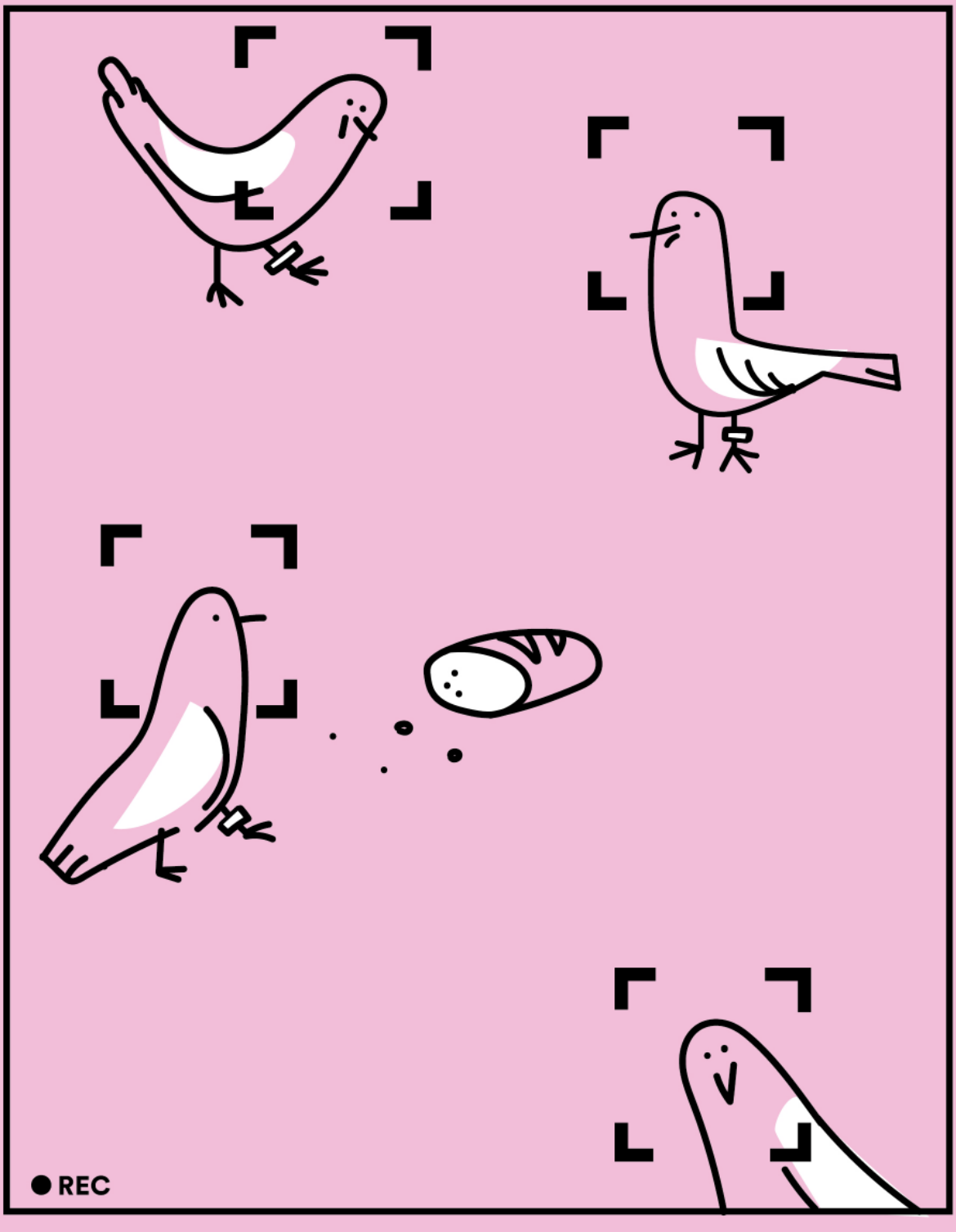
Bureau de dépôt : rue des Bogards 19, 1000 Bruxelles - Périodique trimestriel | Éditeur responsable : Edgar Szoc
53, boulevard Léopold II à 1080 Bruxelles | ldh@liguedh.be | www.liguedh.be | Tél. 02 209 62 80

avril - mai - juin 2023

LIGUE DES DROITS HUMAINS

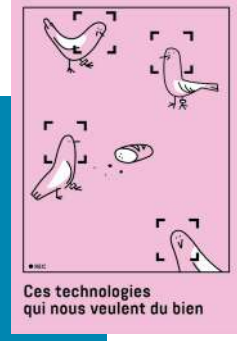
N° D'AGRÉMENT P801323

bpost PB-PP BELGIE(N) - BELGIQUE



Ces technologies qui nous veulent du bien

SOMMAIRE



Coordination
Margaux Hallot

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

Ont participé à ce numéro
Corentin Dubailleul, Elise Degrave, Rémy Farge, Garance Hugo, Clément Martens, Laurent Roy

Relecture
Stéphane De Keyzer, Marie-Carmen De Zaldo, Karine Garcia, Emmanuelle Hardy, Manuel Lambert

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

Édito

Lorsque l'on songe aux enjeux parmi les plus importants liés à la protection des droits humains dans notre pays aujourd'hui, mais aussi demain, l'un des sujets qui s'impose très vite est celui de la prégnance de multiples outils et processus technologiques dans nos vies.
Bien sûr, il y a toujours des personnes qui dorment dans la rue, il y a toujours des sans-papiers violemment expulsés, il y a toujours des personnes détenues dans des conditions indignes, il y a toujours des interventions policières condamnables, il y a toujours des individus discriminés pour de multiples raison, il y a toujours des mouvements de grève pénalisés, il y a toujours un mépris du vivant et de son biotope, et on en passe. Si les questions que soulèvent ces plaies de notre société reçoivent insuffisamment d'attention, il semble en être autrement des défis lancés par les « nouvelles » technologies.

A titre d'exemple, l'émergence vertigineuse de l'intelligence artificielle (IA) et des potentialités qu'elle charrie a suscité de nombreux commentaires quant à son impact, à plus ou moins court ou long terme : les conversations sociales, les articles de presse, les discussions politiques… font état des conséquences jugées tantôt positives tantôt négatives, tantôt les deux, qu'elle comporte.

Il nous a semblé, toutefois, que certains éléments de la discussion en la matière sont largement occultés. En effet, cette technologie, qui n'est pas neutre, comme toute technologie d'ailleurs, vient s'inscrire dans un cadre social et politique existant, avec une série d'effets qu'il est important de ne pas négliger.

Ainsi, le déploiement de ces outils vient ajouter une couche technologique à un tissu de mécanismes et de processus existants. Dès lors, les procédés de surveillance, déjà omniprésents dans nos villes, se voient dotés de potentialités qui alourdissent des craintes déjà exprimées, comme l'illustre le recours massif à la vidéosurveillance de l'espace public, au moyen de caméras dotées de dispositifs « intelligents » à l'efficacité toute relative (C. Debailleul) et/ou aux possibilités inquiétantes (G. Hugo).

De même, le recours aux algorithmes s'insère dans des pans de plus en plus larges de la société, accentuant des inégalités existantes ou en en créant de nouvelles, comme l'illustre le contrôle algorithmique de la fraude sociale (E. Degrave, C. Martens et L. Roy) ou encore le développement de « smart cities » qui laissent sur le bord de la route de nombreux·ses habitant.es de nos villes, particulièrement vulnérables. Au niveau judiciaire, également, l'outil technique promet des jours radieux aux magistrat.es, avocat.es et entreprises, leur permettant de « prédire » l'issue d'une procédure, mais en présentant le risque de renforcer une inégalité des armes déjà à l'œuvre entre différent·es acteurs et actrices judiciaires (R. Farge et E. Hardy).

Notons cependant que, si ces mutations semblent à d'aucun·es inéluctables, nous estimons qu'il n'en est rien. Par exemple, la LDH et ses partenaires ont récemment obtenu du Parlement bruxellois une audition sur la question du recours à la reconnaissance faciale dans l'espace public afin de susciter un débat politique totalement absent en la matière (A. Wavreille). C'est peu face à l'ampleur des enjeux. Mais c'est un premier pas pour atteindre un objectif fondamental : ne pas nous laisser submerger par des évolutions qui n'en ont parfois que le nom et reprendre en main notre capacité de réflexion et d'action.

Manuel Lambert, juriste de la Ligue des droits humains

Aline Wavreille, chargée de communication à la Ligue des droits humains

Reconnaissance faciale : fuyez, vous êtes filmé·es… et identifié·es

La Ligue des droits humains, avec sept autres associations (la Liga voor mensenrechten, le MRAX, le Collectif Mémoire coloniale et lutte contre les discriminations, Genres pluriels, le CIRé, Tactic et Technopolice) a lancé, au printemps dernier, la campagne #Protectmyface visant à interdire l'usage de la reconnaissance faciale dans l'espace public bruxellois. Cette technologie biométrique n'est pas autorisée en Belgique mais les autorités ont pour projet de s'en équiper, les freins techniques sont contournés, plusieurs tests ont déjà été réalisés. Or, l'usage de la reconnaissance faciale dans l'espace public entravera durablement nos droits fondamentaux.

Caméras, logiciels et base de données

La reconnaissance faciale est une technologie que l'on associe encore parfois à de la science-fiction ou à des outils au service de dictatures lointaines. Pourtant, elle est aujourd'hui à portée de main des autorités belges, qu'elles soient fédérales, régionales ou locales. Toutes les caméras de surveillance peuvent potentiellement être dotées d'un logiciel de reconnaissance faciale. Cette technique d'analyse biométrique utilise les caractéristiques du visage (la longueur du front, l'écartement des yeux, les arêtes du nez, la distance entre la bouche et le nez, etc.) pour identifier une personne. Le système transforme les traits des visages en données biométriques et les compare avec celles qui composent la base de données. Pour utiliser la reconnaissance faciale, il faut donc trois éléments : des caméras, un logiciel de reconnaissance faciale et une ou plusieurs bases de données.

Autorisée ou pas ?

En Belgique, aucune loi n'encadre l'usage de la technologie de la reconnaissance faciale. Étant donné qu'elle est une technologie hautement attentatoire à la vie privée – puisqu'elle consiste à récolter et traiter des données à caractère personnel – elle n'est pas autorisée et doit être donc considérée comme illégale et interdite. Le COC, l'Organe de Contrôle de l'Information policière, épinglait dans son avis[1] concernant une proposition de moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité que : «*Ni la loi sur la fonction de police, ni le Code d'instruction criminelle ni une quelconque autre loi (pénale) spéciale n'offre de lege lata un fondement juridique (suffisant) pour l'utilisation de la FRT dans le cadre de missions de police administrative ou judiciaire*».

Des tests… menés en toute illégalité

Cette technologie n'est pas autorisée mais il existe une volonté politique de lui fournir un cadre légal. La reconnaissance faciale suscite un grand intérêt du côté de la police. Quant à la ministre de l'Intérieur Annelies Verlinden, elle a déjà exprimé à plusieurs reprises sa volonté de permettre aux forces de police d'y avoir recours « pour faciliter, par exemple, la recherche de personnes disparues dont la vie est supposée en danger ». Et la ministre de se référer au cadre européen en cours d'élaboration : l'IA-Act. À la mi-juin, le Parlement européen a voté un texte qui encadrait les technologies de surveillance biométrique et a décidé d'interdire la reconnaissance faciale en temps réel, mais la décision se jouera ensuite dans les trilogues entre Parlement européen, Commission européenne et Conseil européen.
En attendant, la police fédérale a déjà mené plusieurs tests en Belgique qui ont été pour la plupart interrompus par le COC, l'Organe de Contrôle de l'Information Policière, parce que jugés illégaux. (Des tests souvent lancés sans en avoir sollicité l'avis du COC, alors que la loi l'y oblige).

1 https://www.organedecontrole.be/files/DA210029_Avis_F.pdf

Rétroactes. En 2017, puis en 2019, la police fédérale a réalisé des tests à l'aéroport de Zaventem. Ils visaient à repérer des suspects en matière de terrorisme et de criminalité organisée : « Nous allons comparer des photos d'auteurs (de crimes) connus, en des endroits spécifiques, sur place et en temps réel », expliquait à la RTBF la porte-parole de la Police fédérale Sarah Frederickx. En 2020, la police fédérale a également réalisé une septantaine de recherches avec le logiciel Clearview IA, très controversé, dans le cadre de réunions Europol. Une enquête du COC a également été ouverte[2].
Par ailleurs, selon une recherche menée par la KULeuven[3] en Flandre et en région bruxelloise, au moins 5 zones de police locale sur 86 répondantes, disposaient de la reconnaissance faciale en 2021, l'une d'elle affirmant même l'utiliser "souvent à très souvent".
En région bruxelloise, des zones de police utilisent notamment le logiciel "BriefCam", de la société israélienne du même nom, pour analyser, au moyen d'algorithmes, les images des caméras qui filment l'espace public bruxellois. La société BriefCam propose aussi un système de reconnaissance faciale, compatible avec une partie du réseau de caméras à Bruxelles. Il n'y a donc plus de frein "technique" au déploiement de la reconnaissance faciale et une volonté politique forte d'en faire usage dans un futur proche.

Libertés et droits fondamentaux menacés

D'importantes sommes d'argent sont donc investies dans du matériel de vidéosurveillance, l'infrastructure est déployée, puis testée. Quant à la question de l'impact sur la population et les droits des personnes : « Ces questions de droits arrivent toujours dans un second temps », observe Chloé Berthélémy, conseillère politique chez EDRI, European Digital Rights. « Il faut toujours un sursaut soit des organes de contrôle, soit du grand public pour que ces questions de cadre légal et de choix de société soient débattues dans l'arène politique, publique et médiatique. (…) Ces préoccupations cruciales arrivent beaucoup trop tard ».

Or, l'usage de la reconnaissance faciale dans l'espace public comporte des risques importants d'atteinte à la vie privée et à la liberté individuelle. « La technologie de reconnaissance faciale à des fins d'identifications, accoudée à une base de données massives qui répertorierait toute la population, c'est la fin de l'anonymat dans l'espace public », tranche Chloé Berthélémy. « Nous serions constamment identifié·es. Ce dispositif aurait des effets dissuasifs sur les personnes, dans l'exercice de leurs droits fondamentaux : avoir peur d'être fiché·e, simplement en circulant, s'auto-censurer dans ses comportements, comme celui d'aller à une manifestation, fréquenter des lieux de divertissement, etc. ».

« Chilling effect »

En Allemagne, selon EDRI, les autorités de la ville de Cologne ont déployé un système de reconnaissance faciale à proximité de bars LGBTQIA+, de lieux de culte (mosquées, synagogues, etc.) et de cabinets médicaux et d'avocat·es sans aucune justification légitime. « Est-ce que l'État a vraiment besoin de savoir tout cela à propos de nous ? », s'interroge Chloé Berthélémy. « La réponse est non. Le problème, c'est que ce genre de systèmes nous conduit vers ces usages ». Et ces usages produisent ce que l'on appelle un chilling effect que l'on peut traduire par effet dissuasif, paralysant ou « d'auto-censure ». Il a par exemple été observé lors d'une évaluation menée en Grande Bretagne sur l'utilisation de la reconnaissance faciale par la Police métropolitaine de Londres. « L'une des conclusions était l'impact sur la liberté de penser et la liberté de réunion », se souvient Rosamunde Van Brakel, criminologue et professeure à la VUB. « Ces technologies peuvent créer des « chilling effects » que l'on a déjà observés pendant les Jeux Olympiques de Vancouver au Canada en 2010. Des activistes figuraient sur une liste de surveillance et alors qu'ils n'avaient commis aucune infraction, ils étaient repérés dans la foule et étiquetés comme danger potentiel.

Par ailleurs, tou·tes les citoyen·nes ne sont pas égaux·ales face au contrôle social

2 https://www.organedecontrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf
3 https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we

et à la criminalisation des comportements. L'usage de cette technologie risque d'impacter surtout les groupes sociaux particulièrement affectés par la précarité et plus marginalisés : personnes migrantes, communauté LGBTQI+, minorités raciales, personnes sans-abri et de toutes personnes qui pourraient avoir une opinion, une identité, un statut administratif ou tout comportement dans l'espace public déterminé comme « non-conforme » à la norme dominante ou établie. L'expérience menée à Côme en Italie parle d'elle-même, le système de surveillance mis en place par la ville est entraîné pour repérer les comportements d'errance sur la voie publique.

Risques de glissement

Enfin, cette technologie implique d'importants risques : piratages de ces données à caractère personnel très sensibles, erreurs et reproduction des discriminations sexistes ou racistes induites par les conceptions sociales dominantes et les institutions qui les vendent et les utilisent, menace d'un glissement vers une surveillance de masse. Chloé Berthélémy, conseillère politique chez EDRI recadre : « On nous dit que les finalités premières de ce genre de surveillance visent la lutte contre le terrorisme ou la recherche d'enfants disparus. Ce sont tous deux des objectifs légitimes, qui devraient être des priorités. Mais la réalité, c'est qu'une fois les infrastructures mises en place, la pratique nous démontre qu'il y a systématiquement un glissement qui s'opère vers d'autres finalités. Si on vise les terroristes, pourquoi ne pas viser la criminalité grave ? Pourquoi ne pas installer des caméras dans le port d'Anvers pour lutter contre le narcotrafic ? Et puis dans tout le quartier autour ? Cette tentation de rentabiliser l'infrastructure est très présente, c'est très simple d'élargir les objectifs une fois l'exception acceptée : one size fits all ».

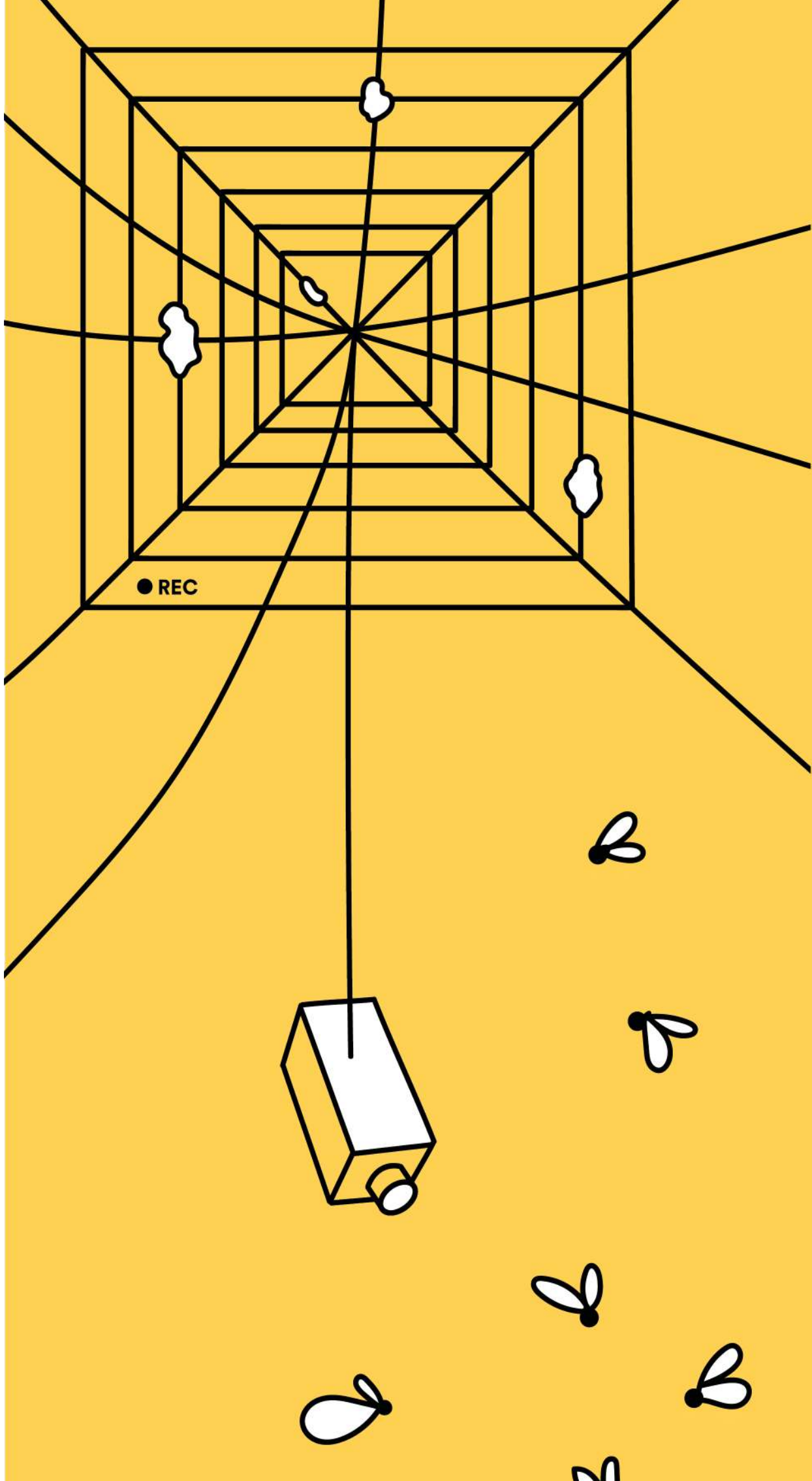
Chine, Iran, Russie, frontières européennes

De plus, l'efficacité de la reconnaissance faciale reste encore très relative en raison des dérives et des erreurs qu'elle engendre encore. En Grande-Bretagne, la reconnaissance faciale est utilisée depuis 2016. Trois ans plus tard, une première étude indépendante[4], réalisée par deux chercheurs de l'Université d'Essex sur l'usage de la reconnaissance faciale par la police de Londres a montré que 80 % des suspect·es signalé·es par le logiciel de reconnaissance faciale étaient en fait innocent·es. Le système identifiait régulièrement des personnes à tort, avec toutes les conséquences sociales et légales que cela peut induire. Les dérives de cette surveillance biométrique sont, par contre, bien documentées. En Chine, la reconnaissance faciale est un outil du contrôle social mis en place par les autorités. Le journal américain Wired révélait il y a quelques mois que l'Iran utilisait la reconnaissance faciale pour identifier les femmes qui refusent de porter le voile. La Russie cible également les opposant·es à la guerre contre l'Ukraine. N'allons pas si loin : l'Union européenne expérimente ces nouvelles technologies dans les hotspots en Grèce et en Italie, ces « camps de réception des migrant·es ». En plus des empreintes digitales des personnes migrant·es, il est prévu de récolter leurs images faciales à partir de 6 ans. Une technologie qui permet également de reconnaître les émotions des demandeur·es d'asile et de mesurer ainsi l'authenticité de leurs récits est testée aux frontières.

Quel modèle de société voulons-nous ?

Les entreprises qui développent ces technologies de surveillance biométrique ont le vent en poupe, elles poursuivent leurs démarches de séduction auprès des gouvernements, des autorités locales, etc. Et souvent, le manque d'expertise et la tentation de céder aux solutions-miracles guident les décisions politiques, qu'importent les risques et les dérives liés à l'usage de la reconnaissance faciale.
Pour la criminologue de la VUB Rosamunde Van Brakel, « *quand les forces de police se préparent à investir dans certaines de ces technologies, une évaluation non seulement légale mais aussi éthique doit avoir lieu. C'est le moment de se demander si l'on veut réellement cette technologie pour notre société. La police ne devrait pas être la seule à prendre cette position, il faudrait également mettre en place un comité éthique avec des représentant·es des communautés locales. J'ai l'impression que la façon dont les technologies sont en train d'être implantées en Belgique est pour l'instant anti-démocratique* ».

4 https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/facial-recognition



Rémy Farge, formateur et Emmanuelle Hardy, conseillère juridique à la LDH

Justice : prédire la place de l'IA

Arriéré judiciaire en augmentation, lenteur des procédures, coût élevé des frais de justice et de défense, etc. Et si la solution résidait dans l'intelligence artificielle ? Les technosolutions gagnent les politiques publiques (libérales) en matière d'écologie, mobilité, sécurité, etc. Et elles comptent bien s'emparer de la justice comme c'est de plus en plus le cas à l'étranger. Elle est dite « prédictive » ou « prévisionnelle », cette justice qui mobiliserait des algorithmes capables de traiter une masse gigantesque de données (législation, jurisprudence et doctrine) afin d'anticiper la décision dans une affaire ou un litige. En gros, l'IA permettrait de prédire la vérité judiciaire à venir sur base des décisions passées. Mais qu'en est-il de l'avènement de la « justice prédictive » en Belgique ?

Face à ce marché potentiellement juteux, de nombreuses legaltechs - entreprises technologiques dans le secteur juridique – vendent des « solutions » aux avocat·es leur permettant de s'épargner les fastidieuses recherches dans les bonnes vieilles bases de données jurisprudentielles et d'anticiper l'issue probable d'un litige ou les chances de succès d'une action. Aux juges, l'on vend l'ambition d'exposer les décisions que d'autres juges auraient prononcées, de répondre à des questions les aidant à prendre leur décision ou prédire le risque de récidive.
En 2018, un projet pilote lancé à Mons à l'initiative du bâtonnier M. Haenecour visait à expérimenter le logiciel Legal Insight développé par Wolters Kluwer Belgium. Utilisés en droit du travail, les traitements algorithmiques concernaient spécifiquement des questions de rupture des relations de travail. Selon Olivier Haenecour, l'utilisation de ce logiciel était encore assez proche de celle d'une base de données classique et le nombre de décisions (environ 36 000) mobilisées pour ce logiciel, trop faible, à son plus grand regret.

Sans accès aux data judiciaires, les legaltechs face à un os

L'élément incontournable à la création de logiciels supposés prévoir l'issue d'un litige ou apporter des arguments pertinents à sa défense réside dans la possibilité d'avoir accès et de pouvoir traiter un très grand nombre de décisions de justice passées. Pour cela, il faut donc que les décisions des cours et tribunaux du pays soient compilées et accessibles. Or, jusqu'à présent, une telle base de données n'existe pas en Belgique mais une loi du 16 octobre 2022 vient précisément d'encadrer la création d'un Registre central pour les décisions de l'ordre judiciaire. Tous les jugements et arrêts prononcés par les juridictions belges seront, à terme, compilés dans cette base de données sous une forme pseudonymisée. Une solution qui a le mérite de concilier le principe de publicité des jugements, favorisant ainsi l'accès au droit et la transparence de la justice, et le respect de la vie privée des justiciables.

Seulement voilà, la loi ne permet l'exploitation des données que par les magistrat·es. Pas par des acteurs tiers tels que des éditeurs et autres entreprises qui se lancent depuis plusieurs années dans le développement de logiciels de justice prédictive. Cet obstacle majeur pour les entreprises intéressées par le marché belge laisse aussi un goût amer à certains praticiens du droit tel que Jean-Pierre Buyle, avocat et ancien président d'Avocats.be. Interviewé par la RTBF, il jugeait cet obstacle « extrêmement regrettable » car « ça ne permet pas de traiter la jurisprudence dans un but d'outil de management, d'outil de prédictivité » [1]. Un tel outil permettrait selon lui d'anticiper les chances de succès d'un litige, et donc de conseiller des clients avant l'introduction d'un éventuel recours. Empêcher le traitement de cette base de données constitue un barrage au développement d'outils de justice prédictive, et frustre en même temps les professionnels promoteurs de ces « solutions » et les entreprises intéressées par le marché belge. L'idée du progrès que représenteraient ces technologies est d'ailleurs souvent appuyée par des arguments purement économiques. Openjustice.be s'inquiète, par exemple, d'« une mort certaine de toute possibilité de développement d'un secteur legaltech belge performant et concurrentiel »[2].

La loi dans le viseur des avocats promoteurs de la justice prédictive

Deux dispositions agacent les avocat·es qui, représenté·es par l'OBFG et l'OVB, ont introduit un recours en annulation devant la Cour constitutionnelle. Il vise, d'une part, l'interdiction du téléchargement massif et le traitement d'un ensemble de données enregistrées dans le Registre central. Cette interdiction empêche toute entreprise, notamment les éditeurs, d'accéder aux données jurisprudentielles utiles au développement d'algorithmes par les legaltechs intéressées par le marché belge. C'est cela qui est pointé lorsqu'on parle d'un système d'« open access » sans « open data ». D'autre part, cette même loi prévoit que « les données d'identité des magistrat·es, des membres du greffe et des avocat·es ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées. » Là encore, le législateur écarte explicitement toute possibilité d'outil prédictif en empêchant notamment la possibilité d'analyser et de traiter des décisions en fonction des magistrat·es.

Des principes en conflit, des professions aussi

L'exposé des motifs de la loi précise que le développement et l'entraînement d'algorithmes ne sont envisagés qu'en soutien des magistrat·es dans l'exécution de leurs missions légales, c'est-à-dire dans une perspective d'aide à la décision. La volonté de maintenir le rôle central du juge malgré l'intervention d'un outil informatique voire d'algorithmes est sans équivoque. Quant au recours à des techniques de traitement du langage naturel[3], il n'est envisagé par le législateur qu'afin de faciliter le travail de recherche, faire du lien avec d'autres bases de données ou encore créer automatiquement des synthèses de décisions. Impossible de ne pas penser au juge colombien Padilla García qui est le premier à avoir utilisé ChatGPT en février pour trancher un litige.[4]

Les avocat·es, ou du moins les plus convaincu·es par la justice prédictive, se sentent laissé·es pour compte face aux magistrat·es. Entendu au parlement, Avocats.be demandait notamment que les avocat·es bénéficient de la possibilité d'exploiter la base de données en construction par le biais de l›intelligence artificielle au même titre que les magistrat·es, en vain. Dans les affaires pénales, Avocats.be estime que le fait que les magistrat·es du parquet puissent avoir accès à un outil qui n'est pas accessible à la personne poursuivie ou à son avocat·e est contraire au principe d'égalité des armes. Ce principe, qui découle du droit à un procès équitable, peut tout autant être invoqué contre l'utilisation de l'IA par les magistrat·es et les avocat·es.

1 https://www.rtbf.be/article/bientot-possible-de-consulter-les-jugements-sur-votre-ordinateur-tablette-ou-smartphone-le-parlement-donne-son-feu-vert-11085642
2 https://openjustice.be/2022/11/21/face-aux-retards-de-sa-digitalisation-la-justice-recule/
3 Cette technologie permet aux machines de comprendre le langage humain grâce à l'intelligence artificielle.
4 Les questions posées à ChatGPT – et dont les réponses figuraient dans le jugement - portaient sur la jurisprudence de la cour constitutionnelle colombienne et sur l'obligation de l'assurance de couvrir tous les coûts liés aux traitements médicaux de l'enfant.

En effet, les algorithmes sont tout à fait opaques et le processus amenant à un résultat ne peut être expliqué avec précision, ce qui risque d'empêcher la bonne compréhension d'un jugement ou sa motivation[5]. Certain·es avocat·es craignent par ailleurs que seuls les cabinets les plus riches puissent se permettre de se procurer ces systèmes.

Si le progrès était conservateur ?

Les discours entourant le déploiement d'une intelligence artificielle capable d'appréhender une masse gigantesque de données afin d'anticiper la décision dans une affaire ou un litige sont assez séduisants : uniformité territoriale des décisions, égalité de traitement des justiciables, sécurité juridique, célérité, réduction des coûts. Cependant, tout récit basé uniquement sur la science et le progrès occulte une réalité à nuancer. Se précipiter vers des réponses technologiques appauvrira immanquablement le débat et les actions politiques pour pallier le manque de moyens de la justice et d'accessibilité pour le justiciable.

Entre les biais algorithmiques de leurs concepteurs et la sur-représentation de personnes d'origine étrangère dans les statistiques pénales due à des discriminations historiques, le risque de reproduire voire d'amplifier ces discriminations est réel. L'exemple du logiciel Compas utilisé par des juges états-uniens pour évaluer le risque de récidive des prévenus est presque caricatural tant les erreurs et les discriminations qu'il provoqua était grossières. On constata notamment une surévaluation du risque pour les afro-américains et une logique inverse pour les blancs. Le principe même de l'usage d'outils prédictifs dans la justice pose un problème fondamental que résume bien le magistrat français Jean-Claude Marin : « *la Justice ne peut être prédictive que par l'analyse de décisions passées offrant la probabilité d'une solution donnée. Autant dire que, paradoxalement, cette justice du futur est éminemment conservatrice.* »[6] Elle occulte par ailleurs l'essence de la mission des juges, qui consiste à confronter les faits au droit dans le but de rendre une justice adaptée tant aux situations particulières qu'aux évolutions de la société.

Un chemin parsemé d'algorithmes ?

Nous l'avons vu, l'avènement de la justice prédictive en Belgique n'est pas imminent. Cependant, si les chances de concrétisation d'une justice entièrement robotisée sont pour l'instant très limitées, le marché de son automatisation regorge de territoires à conquérir : répartition des affaires introduites au sein des greffes, attribution aux différentes chambres des tribunaux, aide à la recherche, au traitement des dossiers administratifs contentieux, recommandation de solution juridique sont autant de perspectives d'informatisation de la justice qu'il convient d'anticiper afin de les encadrer légalement. C'est pourquoi les principes sous-tendant des mécanismes de contrôle démocratique des logiciels publics automatisés se dessinent. Mais promouvoir le développement de l'intelligence artificielle tout en cherchant à nous protéger des risques et dérives est difficilement conciliable. La mise en débat de l'introduction de l'intelligence artificielle dans la justice doit se faire avant que les ambitions économiques ne prennent définitivement le pas sur les enjeux sociaux. Et pour l'heure, les dysfonctionnements qu'engendrent le sous-financement de la justice, son coût pour les justiciables et l'augmentation des seuils d'accès à l'aide juridique, ainsi que la suppression de certaines justices de paix restent prégnants…

5 *Intelligence artificielle et justice : un respect des droits de l'homme par un robot est-il possible ?*, Essai réalisé par Mehdi Amine dans le cadre du concours organisé par le Conseil Supérieur de la Justice, 2021.
6 J.-C. Marin, La Justice prédictive, Colloque la Justice prédictive, 12 févr. 2018 (https://www.courdecassation.fr/toutes-les-actualites/2018/02/12/la-justice-predictive-0)

Corentin Debailleul, chercheur en géographie urbaine (IGEAT-ULB)

Vidéosurveillance à Bruxelles : installer des caméras, mais pourquoi ?

Dans les rues de Bruxelles, le réseau de caméras de surveillance s'est considérablement élargi ces dernières années. Lutte contre l'insécurité et le terrorisme ou contre les dépôts clandestins, régulation du trafic routier, zone de basses émissions, cet outil de surveillance apparaît souvent comme la solution-miracle aux problèmes qui se posent aux autorités. Dans cet article, nous allons tenter de comprendre à quoi servent ces images capturées par les caméras de surveillance, comment elles sont utilisées et remplissent leurs promesses.[1]

Comment la vidéosurveillance s'est-elle développée ?

Connaître le nombre de caméras publiques est plus compliqué qu'il n'y paraît, tant les autorités qui installent ces yeux électroniques sont diverses : zones de police, communes, administrations bruxelloises, etc. La volonté de transparence sur cette question est aussi très aléatoire, comme l'expérimente actuellement la Ligue des droits humains dans le cadre de sa campagne de demandes d'informations sur les dispositifs de surveillance.[2] Néanmoins, on estime qu'il existe, en vrac, à Bruxelles : des dizaines de caméras pour la propreté ; environ 500 caméras dédiées à la circulation ; 300 pour la zone de basses émissions ; plus de 1000 pour la police locale ; et plusieurs milliers dans les stations et les véhicules de la STIB.

À Bruxelles, ce réseau de caméras de surveillance a grandi par à-coups, tantôt à l'occasion d'évènements sportifs d'envergure, tantôt lors de faits divers ou attentats suscitant un choc émotionnel fort. Si les premières caméras apparaissent dans les années 60 du côté de la STIB, c'est l'Euro de football en 2000 qui va jouer un rôle d'accélérateur. Ensuite, en 2003, la région bruxelloise décide de consacrer un budget d'un million et demi d'euros pour équiper les communes de caméras. Le réseau de caméras de police se développe alors pour quadrupler entre 2006 et 2016.[3]
Au milieu des années 2010, alors que la Région promeut la « smart city » et l'installation de capteurs de toutes sortes, les attentats au métro Maelbeek et à l'aéroport de Zaventem viennent plaider pour l'installation de plus de caméras, à plus haute définition. Plus question de se contenter des images floues d'un mystérieux « homme au chapeau » dont on perd rapidement la trace à sa sortie de l'aéroport. S'ensuit également un plaidoyer pour le déploiement de caméras capables de lire les plaques d'immatriculation, dites ANPR (pour *Automatic Number Plate Recognition*). Le discours anti-terroriste s'hybride alors avec des considérations sanitaires et environnementales : la pollution atmosphérique à Bruxelles cause de graves maladies respiratoires et la circulation automobile est pointée du doigt. La Région décide donc de mettre en place une « zone de basses émissions » qui exclut de son territoire, sous peine d'amendes, les véhicules les plus anciens, en commençant par les diesels.[4] Pour ce faire, des centaines de caméras ANPR sont déployées depuis 2018, capables de comparer les images captées dans la rue avec le registre national des immatriculations.

1 Merci à Aline Wavreille pour l'aide apportée à la rédaction de cet article.
2 https://transparencia.be/user/ligue_des_droits_humains
3 Pauline De Keersmaecker et Corentin Debailleul (2016), « Répartition géographique de la vidéosurveillance dans les lieux publics de la Région de Bruxelles-Capitale », *Brussels Studies*, Numéro 104, 2016.
4 https://lez.brussels

VERS UNE GÉNÉRALISATION ?

Les images vidéo qui sont enregistrées par les caméras qui quadrillent le territoire bruxellois circulent ensuite sur des réseaux de fibre optique, appartenant soit aux zones de police, soit au réseau IRISnet mis en place par la Région en partenariat avec Orange. Via ces réseaux, les images convergent vers deux endroits : la première destination relève du dispatching de chaque zone, où une série de policiers est face à un mur d'écrans et en lien avec les patrouilles de terrain ; la seconde destination est « safe.brussels » organisme responsable du centre de crise régional et de la plateforme de « mutualisation de la vidéoprotection ». Cette plateforme permet aux différents acteurs publics comme la STIB, le Port de Bruxelles ou le Ministère des transports de partager leurs images entre eux mais surtout de donner à la police un accès immédiat à l'ensemble du réseau.

Malgré cette tendance à la régionalisation, d'un point de vue géographique, le déploiement de la vidéosurveillance à Bruxelles est loin d'être uniforme. La majorité des caméras se trouve dans le centre-ville de Bruxelles, en particulier dans les espaces commerciaux et touristiques. Ensuite, plus on s'éloigne de ce centre et moins on dénombre de caméras. Cette diminution se fait néanmoins de manière très inégale : en allant vers les quartiers plus aisés du sud-est (Boitsfort, Auderghem, Woluwé, etc.) on trouve beaucoup moins de caméras que si on se dirige vers le nord-ouest, et notamment vers les quartiers populaires jouxtant le canal comme Cureghem ou Molenbeek, qui sont, eux, particulièrement vidéosurveillés.

POUR QUELLE EFFICACITÉ ?

Une caméra conçue pour être placée dans l'espace public et résister aux intempéries comme au vandalisme coûte plusieurs milliers d'euros. À ce montant, il faut généralement ajouter d'autres dépenses, telles que la consultance, l'installation, le fonctionnement et la maintenance. Au total, il faut compter entre 20 000 et 50 000 euros de frais par caméra, sans compter le personnel nécessaire pour visionner ou traiter les images. Dans la mesure où les plans d'installation de caméras publiques comptent souvent plusieurs dizaines voire centaines de caméras, les budgets se comptent en millions d'euros. La vidéosurveillance représente donc un coût très important et pèse lourd sur les finances publiques, notamment locales. Pourtant, les études s'accordent à dire que les caméras sont loin de remplir leurs promesses. Les effets sont généralement considérés comme minimes, voire nuls, à de rares exceptions près.[5] La question dès lors serait de comprendre pourquoi les communes, la Région et zones de police continuent d'investir dans cette technologie ? La réponse est sans doute avant tout politique : notre hypothèse est que faute de pouvoir s'attaquer réellement aux problèmes sociaux, les autorités doivent bien montrer qu'elles agissent pour lutter contre le sentiment d'insécurité…

DES CAMÉRAS « INTELLIGENTES » ?

Pour contrer la critique de l'inefficacité des caméras, les fabricants ont proposé aux autorités publiques des logiciels d'analyse d'images. Une fois enclenchés, ces logiciels vont sélectionner des séquences jugées « problématiques » et envoyer des alarmes en cas de dégagement de fumée, de tag, de dépôts d'immondices, de gens qui courent ou qui errent près d'une voiture, etc. En région bruxelloise, la police utilise un logiciel fourni par la société montoise ACIC pour l'analyse des images en direct. En pratique, ces séquences jugées problématiques par le logiciel sont innombrables sur un territoire aussi large que Bruxelles, la police est alors submergée et dans l'impossibilité d'agir à chaque alarme, d'autant plus que les « faux positifs » sont nombreux. Mais la police utilise un autre type de programme pour faire de l'analyse *a posteriori*, dans le cadre d'enquêtes, par exemple. Le plus souvent, il s'agit du logiciel BriefCam, développé en

5 Élodie Lemaire (2019), *L'œil sécuritaire : mythes et réalités de la vidéosurveillance*, Paris : La Découverte.

Israël. Celui-ci propose un « résumé » de ce qu'une caméra a enregistré durant plusieurs heures. Il permet ensuite de trier les évènements sur base de critères de recherche comme la couleur des vêtements ou le genre d'un·e suspect·e.

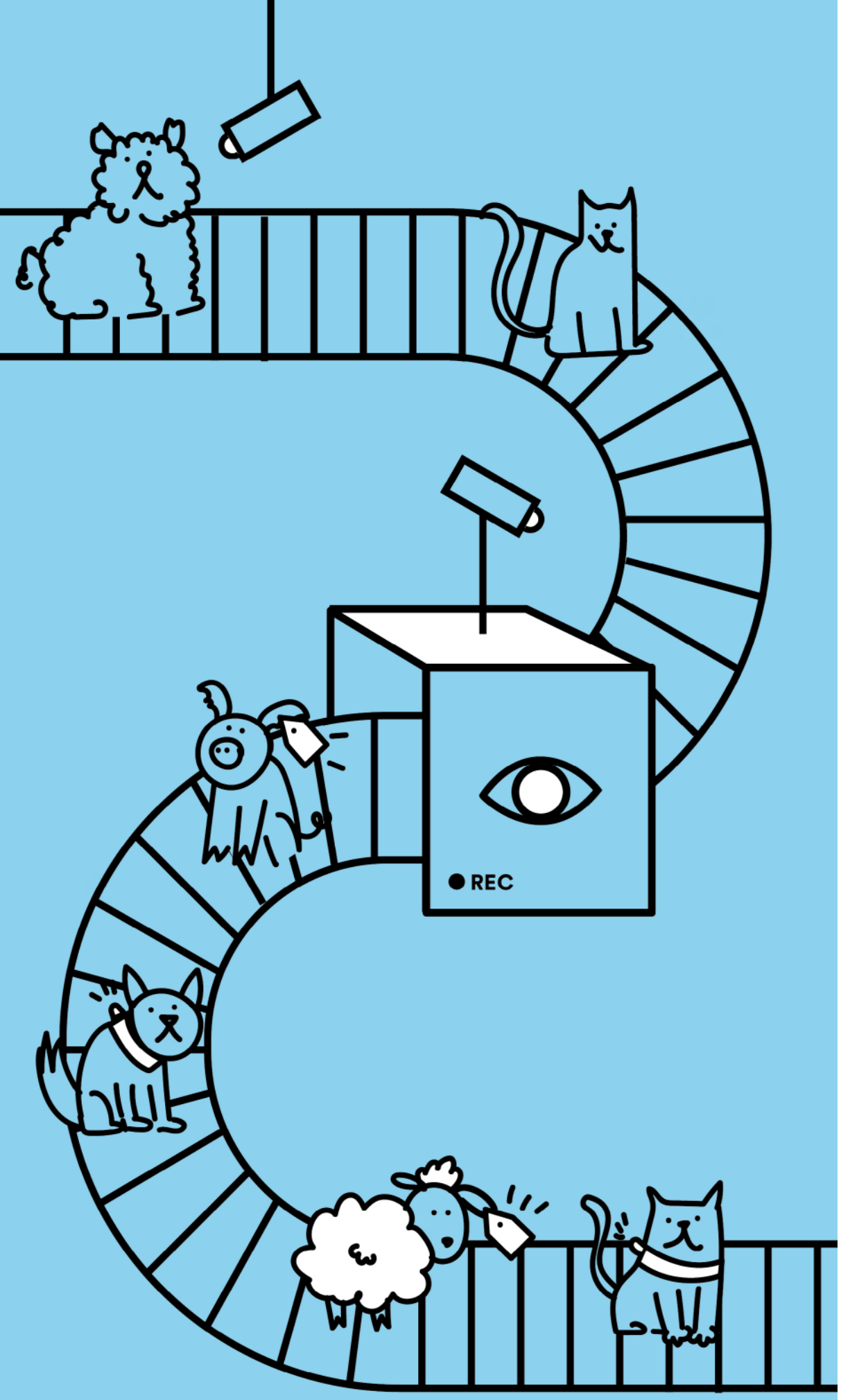
Si ce second logiciel semble plus efficace, il n'en soulève pas moins des questions démocratiques. Tous ces programmes sont basés sur des algorithmes dont le code informatique est fermé, c'est-à-dire protégé par la propriété intellectuelle. Il est donc impossible d'en connaître le fonctionnement réel. Une partie du fonctionnement de la police est donc conditionné par les boites de développement informatique, leurs ingénieurs et les possibilités techniques actuelles, sans qu'il soit réellement possible de remettre en question leurs pratiques. De plus, même si le code était disponible et qu'il y avait une volonté d'en débattre, il ne serait pas forcément possible d'en comprendre le fonctionnement dans la mesure où de plus en plus d'algorithmes sont dorénavant produits par *machine learning*, c'est-à-dire en les entrainant sur des séries de données. À la propriété intellectuelle s'ajoute alors l'opacité du procédé, faisant du fonctionnement de tels dispositifs de véritables « boites noires ».[6] Résultat, on se retrouve souvent avec des logiciels qui reproduisent des dominations raciste ou sexiste, sans qu'il soit facilement possible d'en comprendre la source et de remédier au problème.

Dans la mesure où tout dispositif de surveillance a besoin de code pour fonctionner, la question de la sécurité des dispositifs utilisés se pose également. Des inquiétudes existent quant aux caméras chinoises disponibles à bas coût, mais dont il n'est pas certain que les données qu'elles récoltent ne sont pas envoyées vers la Chine. La Sûreté de l'État recommande donc aux pouvoirs publics de ne pas dépendre des géants du numérique chinois pour leurs infrastructures sensibles. Mais comme me le confiait le responsable de l'informatique d'une zone de police bruxelloise : « on a bien conscience que le problème est le même avec la technologie américaine, mais à choisir… »

A QUOI ALLONS-NOUS FAIRE FACE ?

Les dispositifs publics que l'on croise le plus souvent en rue ont une forme de dôme et sont généralement placés à cinq ou six mètres de hauteur, accrochés aux façades ou perchés sur des poteaux. Ces caméras balaient les espaces qu'elles surveillent et suivent généralement une séquence programmée à l'avance. Les agents peuvent en prendre le contrôle et orienter ces caméras, dans le cadre de manifestations par exemple. De plus en plus, les caméras sont disposées de manière à pouvoir capturer le visage des passants. Elles sont placées à hauteur du regard pour prendre des images dans un angle permettant l'identification. Ce changement d'approche est particulièrement visible dans les gares où, comme vous l'aurez peut-être remarqué, il est maintenant impossible d'entrer, de prendre un escalator ou de regarder les horaires sur les panneaux d'affichage sans se retrouver nez-à-nez avec une caméra. La police procède de façon similaire en installant des caméras fixes à haute définition face aux sorties de métro. Cette évolution est particulièrement inquiétante quand on sait que la direction de la SNCB ou le Ministère de l'Intérieur ont déjà communiqué par le passé leur volonté de recourir à des logiciels de reconnaissance faciale ; que cette fonctionnalité est proposée par le logiciel BriefCam ; et que la police fédérale a déjà été prise la main dans le sac à expérimenter la reconnaissance faciale hors de tout cadre légal…

6 Frank Pasquale (2015), *The Black Box Society, les algorithmes secrets qui contrôlent l'économie et l'information*, Fyp éditions.



Elise Degrave[1], Clément Maertens[2] et Laurent Roy[3]

Les droits fondamentaux face aux algorithmes du secteur public[4]

Les pouvoirs publics n'échappent pas à l'usage des technologies, notamment les algorithmes, pour faciliter certaines tâches. La gouvernance algorithmique, que l'on entend ici comme l'utilisation des algorithmes dans l'exercice du pouvoir, affecte de façon inédite les libertés citoyennes.

Des spécificités dans le secteur public

Promesse d'efficacité pour l'agent de l'administration et de simplicité pour l'administré, la réutilisation des données des citoyen·nes via des algorithmes est de plus en plus fréquente au sein de l'administration et de la police. En Belgique, citons par exemple l'utilisation policière de la reconnaissance faciale pour identifier des suspects[5], les algorithmes utilisés en Communautés française[6] et flamande[7] pour répartir les élèves dans les écoles secondaires, le ciblage des fraudeur·euses sociaux·ales opéré par le logiciel OASIS[8], la détection des domiciliations fictives sur base des données de consommation d'eau, de gaz et d'électricité des assuré·es sociaux·ales[9], ou encore la création de l'immense base de données biométriques européenne Eurodac pour la gestion de la crise migratoire[10]. Derrière leur caractère anodin, ces dispositifs sont en réalité porteurs de grands risques pour les droits fondamentaux, parmi lesquels on retrouve la discrimination des individus, la dégradation de leurs conditions de vie, ou encore l'atteinte à leur liberté de circuler, de manifester, de s'exprimer et d'être protégé dans leur vie privée et familiale[11].

À la différence du secteur privé, le déploiement de ces technologies est **contraignant** dans le secteur public. Là où les citoyens peuvent refuser de se créer un compte Instagram, ils n'ont pas d'autre choix que d'inscrire leurs enfants à l'école, de demander des allocations familiales, ou de décliner leurs identités aux frontières.

Ainsi qu'on l'a dit, certains droits fondamentaux s'en trouvent bousculés, à commencer par le droit à la vie privée. C'est pourquoi des balises doivent être respectées parmi lesquelles la **légalité** qui exige que le Parlement encadre ces outils au terme d'un débat démocratique ayant notamment

1 Professeure à la Faculté de droit de l'UNamur ; Directrice de recherches au Nadi/Crids et à la Chaire E-gouvernement de l'UNamur.
2 Maître en Droit ; Etudiant du Master de spécialisation en droit de l'internet (DTIC) à l'UNamur ; Membre de la Commission Nouvelles technologies et Vie Privée de la Ligue des Droits Humains.
3 Maître en Éthique ; Etudiant du Master de spécialisation en droit de l'internet (DTIC) à l'UNamur ; Membre de la Commission Nouvelles technologies et Vie Privée de la Ligue des Droits Humains.
4 Cet article s'inspire largement du cours de Gouvernance de l'Internet- E-gouvernement de la professeure Elise Degrave, dispensé dans le Master de spécialisation en droit de l'internet (DTIC) à l'UNamur, durant l'année académique 2022-2023.
5 A. Sente, « Reconnaissance faciale : une enquête cinglante sur l'usage du logiciel Clearview par la police », Le Soir, 9 mars 2022.
6 Plusieurs pages du site de la Fédération Wallonie-Bruxelles sont dédiées à expliquer le fonctionnement de l'algorithme mettant en œuvre le décret inscription : https://inscription.cfwb.be/lalgorithme-doptimalisation-des-preferences/, consulté le 19 mai 2023.
7 N. Havermans et T. Wauters, « Simulatie op het toewijzingalgoritme in het secundair underwijs », *SONO*, OL3.2/2, 2020.
8 E. Degrave, « The Use of Secret Algorithms to Combat Social Fraud in Belgium », *European review of digital administration & law*, vol. 1, no. 1-2, 2020, pp. 167-178.
9 Voy. la loi programme du 13 mai 2016 modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale. A ce sujet, voy. E. Degrave, « Contrôle des assurés sociaux et profilage dans le secteur public » J.T., 2015, pp. 517-519.
10 Voy. C. Berthélémy, « Eurodac Database repurposed to surveil migrants », *EDRI*, accessible sur : https://edri.org/our-work/eurodac-database-repurposed-to-surveil-migrants/
11 L. Cluzel, Cours-Conférence donnée dans le cadre de la Chaire Francqui en E-gouvernement de l'UNamur, 10 mars 2023.

permis de peser leurs avantages et inconvénients. Ils doivent également être proportionnés par rapport au but poursuivi. Or, en étant bien souvent présentés comme une simple modernisation de l'administration papier, ces algorithmes n'ont, en réalité, presqu'aucune existence en droit, empêchant les pouvoirs judiciaire et législatif d'exercer un quelconque contrôle.

En outre, le secret qui entoure les algorithmes est problématique au regard du devoir de l'administration de **motiver** ses décisions. Autrement dit, les citoyens doivent être en mesure de comprendre les motifs qui sous-tendent les décisions qui les visent, et les agents de l'administration doivent être en mesure de les leur expliquer. Comment atteindre cet objectif quand on ignore l'existence même d'algorithmes dans le processus décisionnel ?

Le contrôle algorithmique de la fraude sociale

Les problèmes réels dans l'utilisation de ces technologies sont plus nombreux qu'on pourrait le croire. À cet égard, le scandale qui a éclaté aux Pays-Bas est très parlant. Les faits sont les suivants. À partir de 2013, le gouvernement néerlandais décide de s'attaquer davantage aux fraudes aux allocations familiales en se dotant d'un algorithme qui attribue pour chaque citoyen·ne un score de risque en fonction de la probabilité que sa demande d'aide sociale soit frauduleuse. Cet algorithme fonctionne en « boîte noire », c'est-à-dire que personne n'en connait véritablement le fonctionnement. Rapidement, l'administration, suivant aveuglément les préconisations des algorithmes anti-fraude, se met à exiger toujours plus de justificatifs de la part de certain·es allocataires, souvent d'origine étrangère ou vivant dans des quartiers défavorisés. Se voyant dans l'impossibilité de prouver ce que les autorités exigeaient, ces derniers ont dû faire face à des demandes de remboursement d'allocations pouvant s'élever à plusieurs dizaines de milliers d'euros. Au final, entre 25 000 et 35 000 personnes ont été victimes de cette pratique et ont fini noyées sous les dettes[12]. À la suite du scandale, une autorité de contrôle des algorithmes a été instaurée. Depuis début 2023, elle s'assure que les systèmes utilisés par les organismes publics néerlandais respectent les droits humains et qu'ils soient consignés dans un registre public[13].

Un système identique est-il à l'œuvre en Belgique ? Depuis 2005, l'administration belge s'est dotée de l'outil OASIS (Organisation Anti-fraude des Services de l'Inspection Sociale), un algorithme qui utilise les données de différentes administrations fédérales (ONSS, ONEM, SPF Sécurité Sociale, ...) afin de détecter les comportements frauduleux des allocataires sociaux. Problème : c'est l'administration elle-même qui a développé l'outil, sans aucun encadrement juridique, lui permettant ainsi d'éviter un contrôle du Parlement et de la justice. À cause de cette opacité, il est impossible de savoir si ce système est aussi discriminatoire que son homologue néerlandais, sauf à attendre qu'un scandale ne vienne tout dévoiler au grand jour[14].

12 Voy. not. le rapport d'Amnesty international, Xenophobic Machines, 25 octobre 2021, accessible ici :https://www.amnesty.org/en/documents/eur35/4686/2021/en/
; A. Eychenne, « Aux Pays-Bas, un algorithme discriminatoire a ruiné des milliers de familles », Mediapart, 11 novembre 2022, accessible sur https://www.mediapart.fr/journal/international/111122/aux-pays-bas-un-algorithme-discriminatoire-ruine-des-milliers-de-familles?userid=18214e0f-b200-48b4-af66-4e0888cc18c9

13 L. Bertuzzi, traduction d'A. Riffaud, *Les Pays-Bas prennent les devants en matière de supervision des algorithmes*, accessible sur : https://www.euractiv.fr/section/economie/news/les-pays-bas-prennent-les-devants-en-matiere-de-supervision-des-algorithmes/

14 E. Degrave, propos receuillis par P. Laloux, Le Soir, 22 mars 2021, accessible sur https://www.lesoir.be/362211/article/2021-03-22/elise-degrave-aujourdhui-letat-profile-deja-les-belges

La réponse normative en Belgique et en Europe

En septembre 2021, une loi a été proposée en Belgique afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration[15]. L'intention est bonne, mais comme souligné dans l'avis de l'Autorité de Protection des Données, la transparence visée par le projet se limite à révéler le code source de l'algorithme. Même si c'est un bon début vers davantage de transparence, on peut se demander si cette solution sera suffisante pour permettre aux citoyen·nes de comprendre le dispositif technique. La question se pose d'autant plus pour des algorithmes complexes comme ceux de *machine learning*[16]. Comment faire si la publicité ne suffit pas ?

Depuis lors, le 10 février 2023, le Sénat a voté une intéressante proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes[17]. Curieusement, cette initiative a fait peu de bruit autour d'elle, alors qu'elle est particulièrement intéressante dans le contexte actuel.

Par ailleurs, très récemment, le 11 mai 2023, le Parlement Européen a trouvé un accord sur la première législation qui encadrera l'intelligence artificielle[18], l'*AI Act.* Lorsque des systèmes impactent l'exercice des droits et libertés des individus, ils rentrent dans la catégorie des risques élevés, imposant à leurs développeur·euses de respecter certaines exigences de qualité des données d'entrainement, de transparence, et un cadre qui permet une supervision humaine et une responsabilité suffisante. Désormais les autorités qui feront l'usage d'IA à haut risque devront effectuer et publier une analyse d'impact au regard des droits fondamentaux avant de les déployer.

Conclusion

Le secret qui entoure actuellement les algorithmes en Belgique est source d'inquiétude et ne le sera encore que davantage au fur et à mesure que de tels dispositifs se déploieront au sein de l'administration et seront utilisés pour prendre des décisions aussi importantes que l'identification de fraudeur·euses, le refus de droits, le choix d'une école.
Certes, le projet de règlement européen sur l'intelligence artificielle propose des pistes intéressantes. Mais, outre le fait qu'il ne sera pas en vigueur dans l'immédiat, encore faudra-t-il espérer qu'il soit réellement effectif.
En attendant, n'oublions pas que le droit belge peut d'ores et déjà être mobilisé par les avocat·es, les magistrat·es, les associations, les citoyen·nes, pour amener les pouvoirs publics à lever le voile sur les dispositifs algorithmiques et identifier, le cas échéant, leurs effets néfastes. Plutôt que d'attendre qu'un nouveau scandale éclate au grand jour, on ne peut qu'espérer que la Belgique prenne les choses en main, en rejoignant les Pays-Bas dans l'équipe des « bons élèves européens ». À cet égard, la création d'une autorité de contrôle comme celle que l'on retrouve aux Pays-Bas est une idée intéressante pour travailler de concert avec l'Autorité de Protection des Données dans le contrôle effectif des outils algorithmiques.

15 Proposition de loi modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration, *Doc.*, Ch., 55, 2020-2021, n°1904/001.

16 Avis de l'Autorité de Protection des Données n° 157/2021 du 10 septembre 2021.

17 Proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes, *Ann. Parl.*, Sén., 2022-2023, séance du 10 février 2023, n°7-328/4,.

18 Communiqué de presse du Parlement Européen, « AI Act: a step closer to the first rules on Artificial Intelligence », accessible sur : https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

Garance Hugo, stagiaire à la Ligue des droits humains et étudiante en journalisme à l'ULiège

VSA *jacta est*

En France, le projet de loi encadrant les prochains Jeux olympiques et paralympiques de 2024 a mis sur le devant de la scène la problématique de la vidéosurveillance algorithmique (VSA). L'article 10 amorce une première légalisation de cette technologie jusqu'alors utilisée de façon éparse sur le territoire en toute illégalité. La Quadrature du Net[1] , une association qui promeut et défend les libertés fondamentales dans l'environnement numérique, a milité pendant des semaines pour le retrait de cet article et milite encore contre l'expansion de cette technologie de surveillance de masse. Rencontre avec Noémie Levain et Alouette (pseudonyme), membres de l'association.

LA VSA AU CŒUR DE L'ACTUALITÉ FRANÇAISE

Ça y est, c'est officiel : la loi encadrant les Jeux olympiques et paralympiques de 2024 a été promulguée le 19 mai dernier et, avec elle, le fameux article 10 (initialement article 7) qui a particulièrement fait parler de lui ces dernières semaines. Cet article amorce une première légalisation de la VSA en France. Malgré de nombreux plaidoyers en faveur de son abrogation adressés aux institutions et de nombreuses campagnes d'information et de sensibilisation du grand public, la Quadrature du Net n'est pas parvenue à convaincre. Pourtant, pour cette association spécialisée dans les questions juridiques en matière de surveillance de masse, cet article est hors-la-loi.

Mais qu'est-ce que la VSA ?

La vidéosurveillance algorithmique (appelée aussi « augmentée», « intelligente », ou « automatisée ») désigne des dispositifs de vidéosurveillance auxquels sont associés des logiciels algorithmiques. Ces logiciels permettent l'automatisation du travail d'analyse des images. Avec les caméras « classiques » publiques, ce travail est effectué par des humains, des opérateur·rices vidéo au sein des centres de supervision urbains (CSU). Avec la VSA, les logiciels produisent des alertes en temps réel à destination de la police lorsqu'ils détectent un objet, un comportement ou un événement « suspect ». Ils peuvent également effectuer des analyses a posteriori d'archives vidéo. « *On rapproche cela beaucoup de la reconnaissance faciale. Ce sont des technologies qui reposent sur les mêmes algorithmes d'analyse d'images et de surveillance biométrique. La seule différence est que, avec la reconnaissance faciale, on s'attache à regarder un visage tandis qu'avec la VSA, on s'attache à regarder des corps et des comportements.* » (Alouette).

La VSA, comment ça marche ?

Comme pour la reconnaissance faciale, la VSA fonctionne sur des technologies de « *machine learning* » (apprentissage automatique) et, plus particulièrement, de « *deep learning* », c'est-à-dire d'opérations très complexes de calculs en couches de réseaux de neurones. Pour apprendre à l'algorithme à reconnaître une information dans une image ou un flux d'images, il faut le soumettre à une très grande quantité de données. Suivant une logique statistique, l'information sera détectée selon qu'elle présente les caractéristiques « spécifiques » du comportement ou de l'objet que l'algorithme aura appris à identifier. Par exemple, pour reconnaître quelqu'un·e qui court, l'algorithme aura au préalable été soumis à une grande quantité d'images de coureur·euses afin qu'il identifie les caractéristiques spécifiques du comportement « courir », mais aussi à une grande quantité d'images de personnes qui marchent, dansent, nagent, etc., afin qu'il puisse distinguer « courir » de « ne pas courir ».

1 https://www.laquadrature.net/nous/

La VSA en France

La campagne Technopolice lancée en 2019 par la Quadrature du Net – et qui vise à lutter contre l'alliance police-technologie – a permis de lever le voile sur un déploiement en toute illégalité des technologies de surveillance biométriques, en particulier la VSA, sur le territoire français. Depuis 2015, des villes comme Nîmes, Toulouse, Marseille, Paris ou Suresnes, ont développé des projets de VSA dans l'espace public en partenariat avec différentes entreprises de la sécurité (Briefcam, IBM, SNEF, RATP, XXII). Selon Alouette, « *en 2022, il y avait plus de 200 municipalités en France qui utilisaient la VSA alors même que c'est quelque chose d'illégal.* »

Que dit la loi ?

Selon la Quadrature du Net, il y a un grand flou juridique autour des technologies de surveillance. Il existe en France quelques textes généraux qui encadrent la vidéosurveillance dite « classique », le traitement des données personnelles, ainsi qu'une application de la reconnaissance faciale (dans le traitement des antécédents judiciaires), mais rien en matière de traitement algorithmique des images. Du moins, jusqu'à très récemment. L'article 10 de la loi JO 2024 amorce une première légalisation. Pourtant, selon la Quadrature, la VSA est contraire au Règlement général de protection des données (RGPD), qui est une norme européenne, ainsi qu'à la loi Informatique et Libertés. Ces deux textes interdisent le traitement des données biométriques. Or, pour l'association, la VSA est bel et bien une technologie biométrique puisqu'elle permet l'identification d'un individu. La loi JO serait donc, à ce titre, hors-la-loi.

L'INSTRUMENTALISATION DES JO

Selon la Quadrature, le choix des prochains JO comme occasion de légiférer sur la VSA n'est pas anodin. En effet, qui dit événement exceptionnel, dit mesures exceptionnelles, tout particulièrement en matière de maintien de l'ordre et d'intensification des mesures de surveillance. Pour l'association, jouer sur le caractère exceptionnel permet de rendre la pilule plus facile à avaler pour le grand public, alors même qu'aucune étude scientifique ne prouve l'efficience de cette technologie. L'article 10 de la loi JO prévoit, et ce à titre expérimental, que ce traitement algorithmique des images de vidéosurveillance court jusqu'au 31 mars 2025 pour tous les événements sportifs, récréatifs et culturels. L'association parie sur le fait que cet usage « exceptionnel » de la VSA ne sera pas abandonné après cette date.

Une population cobaye

À ce stade, pour la Quadrature, les technologies algorithmiques posent au moins deux problèmes en matière de protection des données personnelles. D'abord, elles vont à l'encontre du principe de minimisation, qui est un principe légal selon lequel la collecte de ce type de données doit être limitée au strict nécessaire. Or, l'entraînement des algorithmes nécessite des millions d'heures d'images de personnes filmées dans l'espace public. En outre, supprimer les données collectées après traitement comme le prévoit l'article 10 de la loi JO ne suffit pas, selon l'association, à les protéger puisque le résultat auquel l'algorithme aboutit sera conservé et pourra servir à une multitude d'applications. Selon Noémie Levain, juriste à la Quadrature, « la phase déterminante, c'est la phase d'apprentissage. À partir du moment où l'algorithme a appris à reconnaître un certain type de comportement ou d'objet dans l'espace public, il existe et pourra être vendu même si on supprime les données traitées. Ce qu'on dénonce, c'est le fait que la population française des JO va être une mine d'or pour ces entreprises. Celles-ci pourront enfin avoir accès aux données et aux caméras de surveillance publiques pour entraîner les algorithmes et se développer sur un marché mondial. »

UNE BOÎTE NOIRE

Un autre problème que met en lumière la Quadrature est que le « raisonnement » opéré par l'algorithme dans l'analyse des données

est inconnu du *data scientist*. Le fonctionnement de l'algorithme est si complexe qu'il demeure opaque même pour l'ingénieur qui le manipule. Celui-ci peut agir sur le résultat, c'est-à-dire corriger les erreurs (confirmer ou non qu'il s'agit d'une personne qui court), mais ne peut maîtriser la manière dont le résultat est créé (comprendre comment l'algorithme a reconnu la personne qui court). « *C'est problématique, explique Noémie Levain, parce que cela veut dire qu'à un moment donné, dans la conception, il y a une boîte noire. À un moment donné, on ne sait pas ce qui se passe. La machine est auto-apprenante.* »
Ce que souligne ici la juriste, c'est que personne ne sait quelles données sont utilisées ni quelles corrélations sont opérées par l'algorithme pour aboutir au résultat. « *Pour opérer des corrélations dans la recherche de quelqu'un·e qui court, l'algorithme peut prendre en compte la gestuelle des personnes, mais aussi leurs vêtements, taille, corpulence, ou couleur de peau. Bref, toutes les données corporelles peuvent être utilisées.* »

Une technologie « neutre » ?

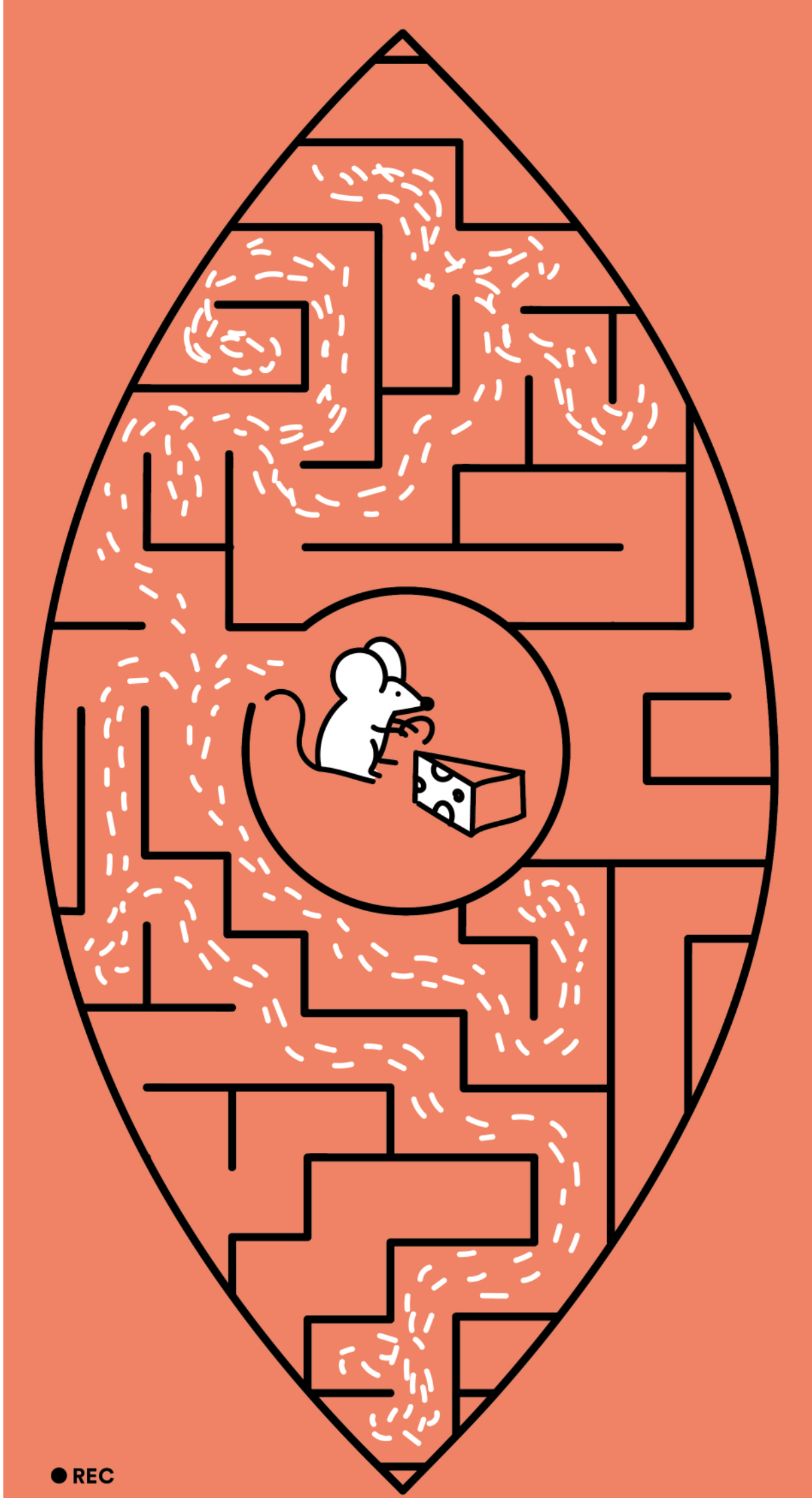
Ce que montre la Quadrature, c'est que, dans le cadre de la VSA, si un algorithme a été entraîné à repérer un comportement suspect à partir d'un jeu de données qui comptent davantage d'hommes, davantage de personnes à la peau foncée, davantage de personnes qui portent un survêtement, par exemple, l'algorithme infèrera qu'être un homme, de couleur, portant un survêtement est un facteur de risque. « *C'est là où, pour nous,* explique Noémie Levain*, tout le fonctionnement des technologies algorithmiques est problématique. C'est pour ça qu'on essaie de contrecarrer les discours qui affirment que la VSA est 'neutre', qu'elle est 'juste une assistante technique', 'juste un outil d'optimisation'. Non, elle renvoie à des choix politiques à tous les niveaux.* »

UN PROJET POLITIQUE : DÉPOLITISER LA SURVEILLANCE ET LA RÉPRESSION

Pour Alouette, ce projet politique de déploiement de la VSA en France relève d'un « *projet sécuritaire qui vise à surveiller et, de là, donner les pouvoirs à la police pour réprimer les populations. On sait, ajoute-t-elle, que l'institution policière est discriminante de manière structurelle. Elle est raciste ; elle va plus souvent réprimer les minorités. Et la VSA va lui donner une sorte d'alibi technique lui permettant de dire : 'ce n'est pas nous qui sommes racistes, c'est l'algorithme qui le dit'. Cette apparence de neutralité est donc hyper dangereuse parce qu'elle va donner beaucoup plus de pouvoirs à l'institution policière. Un plus grand pouvoir de surveillance et de répression donc qui va particulièrement cibler les personnes les plus présentes dans l'espace public.* » *Pour illustrer son propos, Alouette prend l'exemple du maraudage : « Le fait de cibler des personnes statiques, cela cible les SDF et les gens qui font la manche. Réprimer la posture statique, c'est donc réprimer ces personnes-là, ces comportements-là. Ce qui est hyper dangereux.* »

EN CONCLUSION

En France, le marché de la sécurité représentait 1,6 milliard d'euros en 2020. La question des libertés dans l'espace public semble donc subordonnée aux intérêts économiques. La Quadrature du Net déplore cette dépolitisation des technologies de surveillance de masse, et en particulier la VSA. Avec la loi JO, l'association craint un détournement progressif et insidieux de son usage (vers sa généralisation). Une pente dangereuse qui entraînerait un élargissement de la définition des comportements suspects et, ainsi, la criminalisation de nouveaux comportements a priori banals.
« *Ce qui est assez effrayant, conclut Noémie Levain, c'est le niveau de dépolitisation de ces sujets en France. Depuis entre autres les attentats, il y a un contexte sécuritaire qui rend très difficilement audible toute critique des politiques de sécurité et de surveillance. On l'a vu avec la loi JO, critiquer la VSA est perçu comme ne pas vouloir la sécurité, ne pas vouloir la police. Aujourd'hui, il y a zéro réflexion sur la surveillance de masse, sur les pouvoirs de l'État, sur le fait de donner des pouvoirs à la police. Pour le moment, l'État se veut rassurant, il ne légalise que la VSA. Mais cela amorce, je le crains, la légalisation progressive de tout le reste des technologies de surveillance biométrique.* »



Le quizz

Avez-vous bien lu ce numéro ? Nous vous proposons de tester vos connaissances en faisant ce petit quizz ? Prêt·e ?

1. Dans quel pays l'intelligence artificielle a-t-elle déjà été utilisée dans le cadre d'un litige ?

- Mexique
- Colombie
- Argentine

2. Selon les estimations, combien de caméras sont disposées sur le territoire bruxellois pour la police locale ?

- Une bonne centaine
- Un bon millier
- Une bonne dizaine de milliers

3. Quelle ville européenne utilise un système de surveillance afin de repérer les comportements d'errance sur la voie publique ?

- Besançon
- Côme
- San Sebastian

4. Quelle loi vient encadrer la création d'un Registre central pour les décisions de l'ordre judiciaire en Belgique ?

- La loi du 4 juin 2022
- La loi du 25 septembre 2022
- La loi du 16 octobre 2022

5. Combien de municipalités françaises ont eu recours illégalement à la vidéosurveillance algorithmique en 2022 ?

- 2
- 20
- 200

DOSSIER LIBERTÉS PUBLIQUES

6. Le Parlement Européen a trouvé un accord sur la première législation qui encadrera l'intelligence artificielle. Comment s'appelle-t-il ?

- l'AI Act
- l'AI Code
- l'AI Law

7. Depuis quelle année l'administration belge s'est-elle dotée de l'outil OASIS, un algorithme qui utilise les données de différentes administrations fédérales (ONSS, ONEM, SPF Sécurité Sociale, ...) afin de détecter les comportements frauduleux des allocataires sociaux ?

- 2005
- 2010
- 2015

8. Entre 2006 et 2016, le réseau de caméras de police a :

- doublé
- triplé
- quadruplé

9. Comment s'appelle la campagne pour interdire la reconnaissance faciale dans l'espace public bruxellois lancée par la Ligue des droits humains en mars dernier ?

- #Notmyface
- #Itsmyface
- #Protectmyface

10. Dans quel pays un scandale a-t-il éclaté suite à l'utilisation d'un algorithme sensé détecter les fraudes à l'aide sociale ?

- La France
- Les Pays-Bas
- L'Allemagne

Réponses :

1. Colombie
2. Un bon millier
3. Côme
4. La loi du 16 octobre 2022
200
6. l'IA Act
7. 2005
8. quadruplé
9. #Protectmyface
10. Les Pays-Bas

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·ne·s 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 :