TECHNOLOGIES ÉMERGENTES ET INJUSTICE PERSISTANTE

LA DISCRIMINATION ET LA CRIMINALISATION FONDÉES SUR LES DONNÉES DANS LES SERVICES DE POLICE ET PÉNITENTIAIRES EN EUROPE

RÉDIGÉ PAR:

Griff Ferris

Sofia Lyall

FINANCÉ PAR:

European Artificial Intelligence & Society Fund

STATEWATCH

JUIN 2025

Informations concernant la publication

Auteurs : Griff Ferris, Sofia Lyall

Éditeur : Chris Jones

Conception visuelle: McKensie Marie

Ce rapport a pu être publié grâce au soutien de l'European AI & Society Foundation.

Publié par Statewatch en juin 2025.

Soutenir notre travail

N'hésitez pas à faire un don pour soutenir notre travail :

Inscrivez-vous sur notre liste de diffusion :

— **S'inscrire maintenant**

A propos de Statewatch

Statewatch œuvre à publier et à soutenir les travaux de recherche essentiels, les analyses politiques et les travaux d'investigation journalistique afin d'enrichir les débats et d'éclairer les mouvements et les campagnes en faveur des libertés civiles, des droits humains et des principes démocratiques.

statewatch.org
(+44) (0) 203 393 8366
MayDay Rooms, 88 Fleet Street, London EC4Y 1DH,UK

Numéro d'inscription au registre des associations caritatives au Royaume-Uni: 1154784

Numéro d'immatriculation de la société au Royaume-Uni: 08480724

Dénomination de la société enregistrée : The Libertarian Research & Education Trust

Siège social: 88 Fleet Street, London EC4Y 1DH, UK.

Contents

Remerciements

Ce projet a pu être réalisé grâce à la collaboration avec des chercheurs et des organisations partenaires en Belgique, en France, en Allemagne et en Espagne :

— Belgique : Corentin Debailleul, Technopolice Belgique et Ligue des droits humains ;

— France : Edlira Nano et Félix Tréguer, La Quadrature du Net, avec l'aide des membres du groupe de travail Technopolice France de La Quadrature du Net ;

— Allemagne : Sonja Peteranderl, AlgorithmWatch ;

— Espagne : Naiara Bellio en collaboration avec Ana Valdivia et Javier Sánchez Monedero, AlgoRace.

Nous tenons à remercier les personnes et les groupes qui ont contribué à ce projet en participant aux entretiens ou en partageant leurs témoignages, leurs connaissances ou leur expertise.

Nous tenons également à remercier tous les organismes et les personnes engagées dans la lutte contre le racisme et la discrimination au sein des services policiers et du système judiciaire pénal, en particulier dans le contexte de l'émergence récente de ces nouvelles technologies.

Définitions

Intelligence artificielle

La loi sur l'intelligence artificielle de l'Union Européenne définit un système d'IA comme suit :

> *« ... un système automatisé conçu pour fonctionner à différents niveaux d'autonomie, qui peut faire preuve d'une capacité d'adaptation après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, la manière de générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuel. »*[1]

Bien qu'il existe de nombreuses façons de définir l'IA et les systèmes d'IA, c'est cette définition qui est utilisée dans le présent rapport.[2] Il est important de noter que la plupart des systèmes basés sur des données, algorithmiques et automatisés utilisés par les autorités policières et judiciaires en Europe ne font pas appel à l'intelligence artificielle. Certains de ces systèmes utilisent l'apprentissage automatique (voir ci-dessous) qui est un sous-domaine de l'IA. Toutefois, la majorité de ces systèmes utilisent des méthodes statistiques classiques et peuvent être considérés comme des systèmes d'aide à la décision automatisée (voir ci-dessous).

Système d'aide à la décision automatisée

L'Office for AI du Royaume-Uni définit les systèmes d'aide à la décision automatisée comme des outils basés « exclusivement sur des décisions automatisées (sans intervention humaine) » et sur « la prise de décision automatisée assistée (avec intervention humaine) ».[3]

Apprentissage automatique

Le Cambridge Dictionary définit l'apprentissage automatique comme « d'une part, le processus par lequel les ordinateurs améliorent leur propre capacité à effectuer des tâches en analysant de nouvelles données indépendamment de toute intervention humaine sous forme de programmation et, d'autre part, l'étude du développement et de l'exploitation de tels systèmes informatiques capables de fonctionner ainsi ».[4]

La police « prédictive » :

Il existe deux principaux systèmes de police dite prédictive : les systèmes prédictifs fondés sur une approche géographique et les systèmes prédictifs axés sur la personne. Amnesty International définit les systèmes de police prédictive comme suit :

> *«... des programmes informatiques qui s'appuient sur des modèles de données et d'algorithmes pour estimer la probabilité qu'un crime soit commis. Les systèmes de police prédictive calculent des scores de risque qui indiquent la probabilité qu'une personne ou qu'un groupe soit la victime ou l'auteur d'un délit (prédiction basée sur la personne) ou que certains lieux soient propices à la délinquance à l'avenir (prédiction fondée sur une approche géographique). À l'aide de ces scores de risque calculés par ordinateur, les forces de police adoptent des mesures en vue de prévenir ou d'anticiper les faits de délinquance prédits en concentrant leurs efforts sur des zones géographiques, des individus ou des groupes considérés comme à haut risque. »*[5]

Synthèse

La police et le système judiciaire pénal européens utilisent de plus en plus des systèmes et des outils basés sur les données afin de « prédire » où les crimes sont les plus susceptibles d'être commis, de profiler des individus et les classer comme criminels et d'évaluer le « risque » de délinquance ou de criminalité futur.

Ces outils de « prédiction », de profilage et d'évaluation du risque orientent les décisions, les mesures prises par les forces de l'ordre, ainsi que les interventions policières. On peut citer notamment la surveillance et le contrôle, les interrogatoires, les interpellations et les fouilles, les contrôles d'identité, l'interdiction d'emploi, les raids au domicile, les amendes, l'usage de la force, la détention, les arrestations et l'expulsion.

Ces systèmes et décisions fondés sur des données ont également une influence sur les décisions judiciaires pénales, à savoir la détention, la détention préventive, les poursuites, la condamnation et la liberté conditionnelle.

En dehors du système judiciaire pénal, les décisions automatisées peuvent également influencer ou entraîner d'autres types de sanctions, comme par exemple, le refus ou la restriction de l'accès à des services publics essentiels, tels que l'aide sociale et le logement.

Ce rapport fait le point sur plusieurs travaux de recherche axés sur les systèmes d'aide à la décision automatisée et les bases de données utilisés au sein des services de police et du système judiciaire pénal dans

quatre pays : la Belgique, la France, l'Allemagne et l'Espagne. Il est notamment étayé par des travaux de recherche approfondis réalisés par des organisations partenaires basées dans les pays précités.[6] Le rapport se penche notamment sur :

— le processus de création de ces systèmes prédictifs de la criminalité fondés sur des données ;

— leur utilisation par les autorités chargées de l'application de la loi et le système judiciaire pénal ;

— les résultats que ces systèmes génèrent ;

— la manière dont ces résultats sont exploités et influencent la prise de décision, ainsi que les répercussions sur les individus, les groupes et les collectivités.

Il examine également dans quelle mesure ces systèmes ciblent et impactent de manière disproportionnée les groupes et communautés marginalisés, notamment les personnes noires et exposées au racisme, ainsi que les membres de leurs communautés, les victimes de violence basée sur le genre, les migrants, les personnes issues de la classe ouvrière ou de milieux et quartiers socio-économiquement défavorisés, ainsi que les personnes souffrant de problèmes de santé mentale.

La plupart de ces systèmes s'appuient sur des données historiques, issues par exemple des services de police ou du système judiciaire pénal. Ces données révèlent l'existence de biais discriminants passés et présents au sein de ces institutions et de la société en général, ce qui a pour effet d'entraîner une présence policière excessive, ainsi qu'une criminalisation des communautés marginalisées, notamment les migrants, les groupes exposés au racisme ou les habitants de quartiers à faible revenu.

Utilisés dans le cadre du maintien de l'ordre et de la justice pénale, ces systèmes ont d'importantes répercussions sur les libertés individuelles, telles que le droit à une justice impartiale, au respect de la vie privée et à la protection contre la discrimination.

Systèmes de police « prédictive » fondés sur une approche géographique

Des méthodes de police « prédictive » fondées sur une approche

géographique sont actuellement en cours de développement et de déploiement à l'échelle de l'Europe. Ces systèmes algorithmiques ont été conçus pour « prédire » où et quand des délits sont susceptibles d'être commis. Grâce à ces prédictions, les forces de l'ordre peuvent affecter des ressources dans les secteurs visés. Ces outils de prédiction de la criminalité fondés sur une approche géographique sont, ou ont été, déployés dans les quatre pays étudiés : la Belgique, la France, l'Allemagne et l'Espagne, ainsi que dans d'autres pays européens, par exemple : l'Italie, les Pays-Bas, la Suisse et le Royaume-Uni.

Les travaux de recherche ont permis d'identifier deux types principaux de systèmes fondés sur une approche géographique :

— la prédiction des zones de criminalité potentielle ou « points chauds », qui s'appuie sur les données historiques des services de police afin d'anticiper les futurs lieux de criminalité et

— les algorithmes de prédiction des « risques » liés à l'environnement qui reposent sur l'hypothèse selon laquelle les facteurs environnementaux déterminent les endroits où les crimes sont commis, ce qui permet d'anticiper et classer certaines zones comme dangereuses.

Les méthodes de prédiction des « points chauds » de la criminalité se basent sur des statistiques historiques sur le lieu et le moment de la survenue des délits. Elles visent ainsi à prédire les « points chauds » et anticiper les futurs lieux de criminalité. Ces prédictions sont fondées sur l'analyse des données statistiques et des tendances tirées de vastes ensembles de données sur la criminalité, généralement issues de bases de données policières. En règle générale, ces systèmes de prédiction des « points chauds » permettent aux services de police d'obtenir une « carte thermique » des zones ou lieux susceptibles de présenter un taux élevé de criminalité.

Les systèmes de prédiction des « points chauds » de la criminalité permettent d'allouer des ressources policières et de déterminer où et quand patrouiller au niveau des zones identifiées. Dans les zones considérées comme « points chauds », différentes mesures peuvent être mises en œuvre, comme la surveillance, la collecte de données, les contrôles d'identité, les interrogatoires, les fouilles, les ordonnances de protection, les raids au domicile et les interpellations. Les travaux de

recherche ont soulevé certaines inquiétudes, notamment le fait que les secteurs considérés comme « points chauds » de la criminalité sont de manière disproportionnée des quartiers où résident et travaillent des communautés précarisées et exposées au racisme.

Les systèmes fondés sur une approche géographique se nourrissent d'informations relatives à l'environnement et au contexte. Ils se basent sur des éléments environnementaux ou contextuels pour identifier les secteurs ou lieux où le risque de criminalité est perçu comme étant plus élevé. Un algorithme attribue une valeur de vulnérabilité aux lieux en fonction de facteurs spatiaux, tels que :

— l'éclairage public ;

— les arrêts de bus ou de métro ;

— les terrasses de cafés ;

— les fast-foods ;

— les toilettes publiques ;

— les pharmacies, les bars, certains types de magasins ;

— la présence d'arbres ou de bancs ;

— les écoles et les bureaux de poste.

Ce procédé met en évidence les mêmes biais discriminants que ceux que l'on retrouve dans les systèmes fondés sur les données criminelles.

Systèmes de police « prédictive » axés sur la personne et systèmes « prédictifs » de la criminalité

Les outils de « prédiction » de la criminalité axés sur la personne visent à évaluer la probabilité ou le « risque » qu'une personne commette un délit. Des systèmes similaires sont employés pour évaluer la probabilité qu'une personne soit victime d'un crime, comme la violence basée sur le genre, ou pour détecter les faux signalements de crimes.

Les personnes ciblées par ces systèmes font l'objet d'une évaluation continue de leurs informations personnelles, de leurs antécédents, de leur situation actuelle, ainsi que de leur réseau familial et social. Le

but est de comprendre et d'anticiper le comportement, le niveau de dangerosité ou la délinquance présumée de ces personnes, ce qui peut avoir de graves conséquences. Les résultats produits par ces systèmes pourraient mener à la mise sous surveillance de certains individus et entrainer également une augmentation du nombre de contrôles policiers, d'interrogatoires, de perquisitions, de visites à domicile ou au travail, d'interdictions d'emploi, de détentions, d'expulsions ou d'arrestations.

Ces outils sont également utilisés dans le système juridique pénal. Ils peuvent ainsi influencer le processus décisionnel des juges (y compris la détermination de la peine), la durée d'emprisonnement d'une personne, la date de sa libération, ainsi que les conditions de détention.

Conclusion

Le profilage racial et socio-économique, la discrimination et la criminalisation découlent de l'utilisation de tels systèmes. Ces systèmes ciblent en particulier les groupes marginalisés, comme les minorités noires et ethniques, ainsi que les personnes issues de milieux socio-économiques défavorisés.

Leur utilisation entraîne des conséquences inéquitables et discriminatoires : surveillance, contrôles d'identité et fouilles, harcèlement policier, raids au domicile, interdiction d'emploi, arrestations, détentions et expulsions.

Ces systèmes fonctionnent dans l'ombre : les individus concernés ne savent pas qu'ils ont été ciblés et, par conséquent, ne sont pas en mesure de contester les mesures qui en découlent. Même s'ils pouvaient les contester, il n'existe pas de cadre clair en matière de responsabilité.

Les conclusions de tous les rapports des partenaires et du présent rapport sont unanimes : ces systèmes doivent être interdits.

Introduction

Dans tout le continent européen, les autorités policières et judiciaires ont de plus en plus recours à des systèmes numériques et fondés sur des données. Les nouvelles technologies émergent à un rythme effréné, déployées dans une certaine opacité et sans évaluation préalable de leurs impacts et conséquences.

Parmi ces technologies citons :

— la surveillance par reconnaissance faciale ;

— les systèmes de reconnaissance des émotions ;

— les outils d'extraction des données de téléphones portables ;

— le marquage électronique et les bracelets électroniques ;

— les systèmes prédictifs et de profilage.

Ces technologies ont en commun la collecte et l'analyse d'importants volumes de données, souvent des informations personnelles confidentielles, afin d'éclairer le processus décisionnel.

Le présent rapport porte sur les systèmes algorithmiques, fondés sur des données et d'aide à la décision automatisée, utilisés par les services policiers afin de « prédire » où et quand des crimes seront perpétrés, ainsi que le profil des auteurs. Les partisans

de ces approches « prédictives » prétendument scientifiques soutiennent qu'elles permettent aux forces de l'ordre d'optimiser leur efficacité opérationnelle et de réduire les coûts :

> *« En se basant sur une nouvelle stratégie appelée « Evidence-Based-Policing [Maintien de l'ordre fondé sur des preuves] », les gouvernements peuvent collaborer en toute transparence avec la police et le public afin d'investir dans des tâches policières efficaces et rentables. Il est possible de réaliser ces investissements tout en réduisant les budgets de la police, notamment en éliminant certaines tâches policières coûteuses et inefficaces ».*[7]

En effet, le colonel Patrick Perrot, coordinateur de l'IA pour la ***Gendarmerie nationale*** française, a affirmé que les méthodes basées sur les données permettent à la police d'anticiper les crimes avant qu'ils ne se produisent :

> *« ... l'approche scientifique nous permet de développer des techniques de modélisation capables d'appréhender les évolutions à venir et de s'y préparer. La notion d'anticipation est aujourd'hui déterminante dans le domaine de la criminalité ».*[8]

Ainsi, les organisations de la société civile, les militants politiques et les organisateurs, ainsi que le corps enseignant, de toute l'Europe ont à leur tour examiné de plus près les systèmes de police dits « prédictifs ».

Plusieurs groupes ont exprimé de sérieuses inquiétudes quant aux conséquences possibles de ces systèmes, comme par exemple la surveillance, le contrôle, les interrogatoires, les interpellations et les fouilles, les amendes, les raids au domicile, l'usage de la force, les expulsions, la détention et les arrestations, ainsi que les violations potentielles des droits individuels. Ces systèmes mettent en jeu et sont susceptibles d'enfreindre le droit à une justice impartiale, au respect de la vie privée, à la protection contre la discrimination, à la présomption d'innocence et à l'accès à un recours effectif.[9]

Les résultats des travaux de recherche présentés dans ce rapport confirment ces inquiétudes. L'objectif est de soutenir les campagnes internationales, nationales, régionales et locales en vue d'exiger l'interdiction de l'utilisation de l'IA et des algorithmes par le système judiciaire. Dans les pays où aucune interdiction n'a encore été adoptée, il est nécessaire d'instaurer des garanties procédurales, comme des tests rigoureux avant déploiement, la transparence publique et la possibilité de disposer de voies de recours efficaces.

Présentation du rapport

Ce rapport compile et synthétise des études détaillées sur les systèmes « prédictifs » et les bases de données utilisés dans les services de police et les systèmes judiciaires pénaux en Europe. Il se base sur des recherches effectuées dans quatre pays : la Belgique, la France, l'Allemagne et l'Espagne.

Ces pays ont été choisis principalement pour deux raisons. Il était bien connu que les systèmes « prédictifs » étaient largement employés par les services de police et dans le système judiciaire pénal. Toutefois, peu de recherches ont été publiées sur le développement, l'utilisation et l'impact de ces technologies.

Ces travaux de recherche ont été menés au cours des années 2023 et 2024 par des chercheurs d'***AlgorithmWatch***, de ***La Quadrature du Net et de Technopolice***. Les versions originales sont disponibles en ligne.[10] Des travaux de recherche complémentaires sur l'Espagne ont également été réalisés par ***AlgoRace***.

Dans chaque pays, les chercheurs se sont efforcés de mettre en lumière les systèmes « prédictifs » employés, leur fonctionnement, les résultats générés, ainsi que leurs conséquences sur les individus, les groupes et les collectivités.

Ces travaux de recherche sont regroupés dans le présent rapport afin de fournir une vue d'ensemble du contexte, des tendances et des conséquences découlant de ces systèmes de police « prédictive » mis en œuvre en Belgique, en France, en Allemagne et en Espagne. Le rapport inclut également d'autres études et rapports sur l'utilisation des systèmes prédictifs et de profilage dans les services de police et les systèmes judiciaires pénaux dans d'autres pays d'Europe, notamment les Pays-Bas, l'Italie, la Suisse et le Royaume-Uni.

Le rapport comprend quatre sections qui examinent les systèmes « prédictifs » basés sur des données utilisés par les forces de police : les systèmes fondés sur une approche géographique, les systèmes axés sur les personnes, la vidéosurveillance algorithmique et les bases de données. Chaque section de ce document couvre les objectifs, les données d'entrée et les résultats générés par ces systèmes en se concentrant sur des exemples spécifiques de chaque pays.

La dernière partie du rapport examine les principales inquiétudes et violations des droits individuels, notamment la discrimination, la criminalisation, la transparence, la responsabilité et l'illégalité.

Discrimination structurelle et institutionnelle

La plupart des systèmes prédictifs de la criminalité se fondent sur des données historiques relatives aux infractions. Cela reflète le racisme institutionnel, la discrimination et les préjugés existant au sein des forces de l'ordre, du système judiciaire pénal et de la société en général.

Les pratiques policières discriminatoires de profilage racial et ethnique font, depuis plusieurs années, l'objet de nombreuses critiques par les victimes, les associations de victimes, les universitaires, les organisations de défense des droits de l'homme et les organisations internationales. Ces pratiques se manifestent souvent par des arrestations, des contrôles d'identité et des fouilles motivés par des facteurs tels que la race, la couleur de peau ou l'appartenance religieuse (présumée).

Une étude réalisée en 2017 par l'Agence des droits fondamentaux de l'UE a interrogé des personnes dans les 28 États membres de l'UE (de l'époque). L'étude a révélé que près de la moitié des personnes interrogées appartenant à certaines communautés ethniques minoritaires ont indiqué avoir été interpellées par la police. Il s'agissait notamment de personnes « d'origine africaine subsaharienne » au Luxembourg et en Finlande, de personnes « d'origine nord-africaine » aux Pays-Bas et de Roms en Grèce et au Portugal.[11]

Selon l'Agence des droits fondamentaux (ADF) de l'UE, la majorité des personnes « d'origine africaine » interpellées par la police dans l'UE avaient le sentiment que ces interpellations étaient influencées par des facteurs raciaux.[12] En France, selon le défenseur des droits, les jeunes hommes perçus comme étant des personnes noires ou arabes ont 20 fois (soit 2 000 %) plus de chances d'être contrôlés par la police que le reste de la population.[13]

En Belgique, il y a peu de données officielles sur le profilage ethnique, car la police n'a jamais été tenue de documenter les arrestations et contrôles effectués. Cependant, Amnesty International a interrogé des agents de police belges qui ont reconnu que le profilage racial était une pratique courante au sein des forces de l'ordre. L'un d'eux a même déclaré : « Je me base sur le profilage ethnique, mais je ne sais pas comment je pourrais modifier mes méthodes de travail. Nous devons discriminer, autrement nous n'arrêterions jamais personne ».[14]

En Espagne, la police interpelle et fouille de manière disproportionnée les personnes en fonction de leur apparence raciale, ethnique ou religieuse. Ce fait a été documenté dans de nombreuses études.[15] Les personnes originaires d'Afrique du Nord, d'Afrique subsaharienne et des pays d'Europe de l'Est sont plus susceptibles d'être soumises à des contrôles d'identité que les Espagnols.[16]

En Allemagne, les ressortissants étrangers sont surreprésentés parmi les suspects fichés par la police, les individus condamnés par les tribunaux ou incarcérés.[17] Toutes choses étant par ailleurs égales, en Belgique, une étude a révélé que les personnes jugées portant un nom perçu comme musulman avaient plus de chances d'être condamnées que les personnes ayant un nom perçu comme belge.[18] En France, les ressortissants étrangers ont trois fois plus de chances d'être placés en détention provisoire,[19] tandis qu'en Belgique, 45 % des personnes en détention provisoire ne sont pas des ressortissants belges.[20]

Malgré ces preuves évidentes, la discrimination par la police, les autorités chargées de l'application de la loi et le système juridique pénal n'est toujours pas reconnue comme un problème structurel ou institutionnel dans de nombreux pays européens. Comme le soulignent les auteurs d'Afrozensus 2020 dans une enquête menée en Allemagne auprès de 6 000 personnes noires, d'origine africaine ou issues de la diaspora africaine :

> *« ... il subsiste encore des doutes : le public se pose des questions, à savoir si le racisme institutionnel existe vraiment dans les services policiers allemands ou s'il y a seulement des cas soi-disant isolés. Les personnes noires, africaines et issues de la diaspora africaine ne se posent pas cette question, car pour elles c'est une réalité quotidienne ».*[21]

Ces données, qui révèlent une discrimination systémique et institutionnelle, sont intégrées dans les systèmes « prédictifs », de profilage et d'évaluation des « risques » par les autorités chargées de l'application de la loi et les autorités judiciaires pénales.

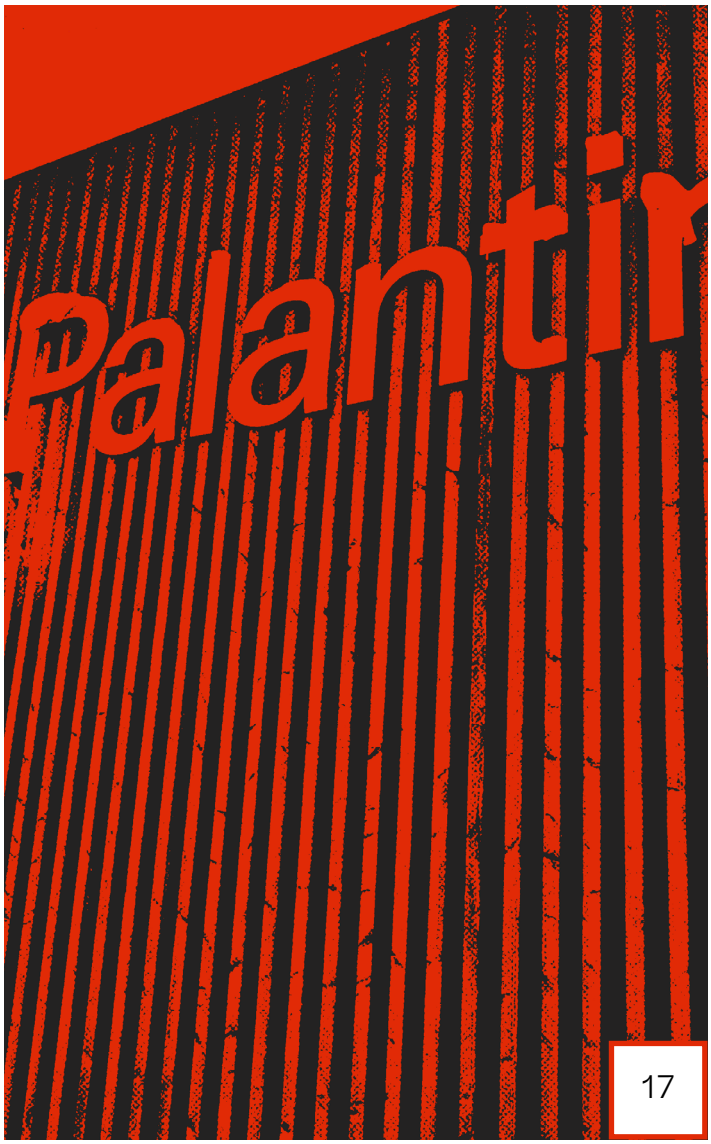
Rôle des entreprises

Les entreprises privées jouent un rôle important dans les processus de numérisation et d'automatisation des services policiers. Les chercheurs ont identifié un grand nombre de systèmes en Belgique, en France et en Allemagne fournis aux forces de police par des entreprises de sécurité privées, généralement dans le cadre d'appels d'offres concurrentiels. D'autres systèmes basés sur des données sont mis au point en interne ou en collaboration avec des chercheurs universitaires.

Palantir est l'entreprise technologique la plus connue et la plus importante qui vend des logiciels de police « prédictive » en Europe. Parmi les 16 États fédéraux allemands, trois exploitent actuellement les systèmes de Palantir.[22] En 2024, le chiffre d'affaires global de Palantir s'élevait à 2,87 milliards de dollars.[23] L'entreprise est réputée à l'échelle mondiale pour ses relations avec les services de renseignement, l'armée et divers autres organismes du secteur public.[24]

Parmi les autres entreprises importantes qui fournissent des systèmes basés sur les données aux forces de l'ordre en Europe, on peut citer :

- Briefcam, une entreprise israélienne qui produit des systèmes de vidéosurveillance basés sur l'IA ;[25]
- ClearView, une entreprise américaine spécialisée dans la reconnaissance faciale qui commercialise principalement des logiciels destinés aux autorités chargées de l'application de la loi ;[26]
- Edicia, une société française qui développe des logiciels de « sécurité urbaine » ;[27]
- Simsi, qui a conclu un partenariat avec l'université américaine Rutgers dans le New Jersey pour commercialiser le système de prévention situationnelle Risk Terrain Modelling (RTM) ;[28]
- La société EuroCop en Espagne, qui a signé plus de 100 contrats avec des



administrations publiques au cours des deux dernières décennies ;[29]

— Securitas, une société suédoise proposant des « solutions de sécurité » ;[30]

— SopraSteria, une entreprise française qui a également signé des contrats avec l'UE pour mettre au point un vaste système biométrique pour la police et les services d'immigration.[31]

Outre Briefcam, d'autres sociétés israéliennes ont signé des contrats avec les autorités belges, à savoir TA9/Rayzone et Interionet. Les origines de la société TA9 sont particulièrement inquiétantes. Le PDG avait occupé le poste de directeur adjoint au sein de l'Unité 8200 qui est l'unité de renseignement de l'armée israélienne supposée être responsable du développement des systèmes d'IA.[32] Plusieurs fonctionnaires qui étaient employés par l'Unité 8200 ont par la suite créé leur propre entreprise spécialisée dans la sécurité.[33]

Le secteur des technologies de surveillance est actuellement en plein essor.[34] Selon une estimation, le taux de croissance annuel mondial de ce secteur serait de 12,5 %. En 2025 ce secteur est donc évalué à 186 milliards de dollars.[35] Compte tenu du potentiel de profit dans ce secteur, il est logique de prévoir au cours des prochaines années une augmentation du nombre de systèmes « prédictifs » et des entreprises qui les fournissent.

La loi sur l'intelligence artificielle de l'Union Européenne

La Loi sur l'IA de l'UE est une norme juridique mondiale de référence visant à réglementer l'IA en tenant compte des dangers éventuels qu'elle pose pour la santé, la sécurité et les libertés fondamentales. Ce texte a été adopté par le Parlement européen à l'issue de

longues et complexes négociations en juin 2024. Les premières obligations imposées par la Loi sont entrées en vigueur en février 2025.

La Loi sur l'IA énonce un certain nombre de « pratiques illégales liées à l'IA ». Parmi ces pratiques citons notamment :

— la « police prédictive » ;

— les systèmes d'identification biométrique à distance (p. ex. la reconnaissance faciale publique) ;

— le « score social » ;

— la reconnaissance des émotions.[36]

Dans le cadre de cette Loi, l'interdiction des systèmes « prédictifs » de la criminalité manque de précision et de clarté. De plus, elle comporte une exception majeure susceptible de réduire significativement son impact. Il est fort possible qu'un grand nombre, voire la totalité, des systèmes couverts dans ce rapport et dans la recherche qui le sous-tend ne soient pas interdits[37] en vertu de cette Loi. En ce qui concerne les systèmes de police prédictive, la Loi interdit :

> *« ... la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation d'un système d'IA pour l'évaluation des risques des personnes physiques afin d'évaluer ou de prévoir le risque qu'une personne physique commette une infraction pénale, sur la seule base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité et de ses caractéristiques ».*

Toutefois, le texte poursuit en disant :

> *« ... cette interdiction ne s'applique pas aux systèmes d'IA utilisés pour soutenir l'évaluation humaine de l'implication d'une personne dans une activité criminelle, qui est déjà fondée sur des faits objectifs et vérifiables directement liés à une activité criminelle ».*[38]

La loi semble interdire ***certains*** systèmes d'IA qui utilisent le « profilage... des traits de personnalité ou des caractéristiques » d'une personne pour prévoir le risque. Toutefois, cette interdiction ne s'applique pas aux systèmes d'IA utilisés pour « soutenir » l'évaluation humaine. Cet ajout en fin de paragraphe a pour effet de vider l'interdiction de toute substance. Les autorités chargées de l'application de la loi peuvent simplement déclarer, comme c'est déjà le cas, qu'elles ont recours à l'IA dans le but de « soutenir » l'évaluation humaine.

De plus, le texte ne fait pas clairement référence aux systèmes prédictifs de la criminalité fondés sur une approche géographique qui sont très répandus en Europe

et ne les interdit pas. Les lignes directrices de la Commission européenne sur les pratiques illégales liées à l'IA indiquent clairement que ces systèmes n'entrent pas dans le champ d'application de l'interdiction.[39] Ces lignes directrices ne sont toutefois pas contraignantes. En cas de litige juridique concernant de tels systèmes, la Cour de justice de l'Union européenne (CJUE) pourrait avoir le dernier mot.

Décrite comme étant « partielle », l'interdiction est nettement moins restrictive que celle initialement approuvée par le Parlement européen en juin 2023.[40] Certains gouvernements européens, ainsi que des multinationales du secteur technologique, ont activement cherché à affaiblir les garanties prévues par la Loi.[41]

La Loi sur l'IA prévoit des dispositions très basiques en matière de transparence. Elle préconise notamment que toute personne concernée doit être informée en cas d'utilisation d'un système d'IA classifié comme étant « à haut risque ».[42] Toute personne visée par une décision prise sur la base de résultats générés par un système d'IA à haut risque produisant des effets juridiques à son égard ou ayant des conséquences qu'elle juge significatives sur sa santé, sa sécurité ou ses droits fondamentaux, est en droit de demander une « explication claire et pertinente » du rôle que ce système d'IA a joué dans la prise de cette décision.[43]

Il y a toutefois une exception majeure concernant les systèmes employés dans le but de détecter, prévenir, poursuivre les infractions pénales et enquêter à leur sujet.[44] Par conséquent, la Loi ne contient aucune disposition visant à accroître la transparence des systèmes de police « prédictive » et prédictifs de la criminalité.

De plus, il n'existe pas de dispositif juridique efficace pour que les personnes affectées par des « pratiques illégales liées à l'IA » ou par des systèmes d'IA non conformes à la Loi puissent contester l'utilisation de tels systèmes ou demander réparation pour le préjudice subi en raison de l'utilisation de tels systèmes.[45] Les personnes concernées peuvent porter plainte auprès des autorités compétentes de leur pays. Toutefois, la Loi ne contraint pas légalement ces autorités à fournir une réparation.[46]

La législation existante sur la protection des données, notamment le Règlement général sur la protection des données (RGPD) et la Directive « Police-Justice » (Law Enforcement Directive, LED), comporte plusieurs normes. Il convient de noter que la Directive « Police-Justice » s'applique à l'utilisation des données et des systèmes d'aide à la décision automatisée par les autorités chargées de l'application de la loi et interdit toute décision prise ***exclusivement*** via un processus automatisé. Toutefois, comme nous l'avons vu précédemment, cela peut vider l'interdiction de toute substance. Les autorités chargées de l'application de la loi pourraient argumenter que le processus décisionnel ne reposait pas exclusivement sur un traitement automatisé.

Méthodologie

Les travaux de recherche sur la Belgique, la France, l'Allemagne et l'Espagne, qui forment la base de ce rapport, ont été réalisés par des chercheurs et enquêteurs basés dans les pays précités, en utilisant diverses méthodes et avec le soutien des rédacteurs de ce rapport :

- ***Entretiens :*** les chercheurs ont mené des entretiens avec des spécialistes, des universitaires et d'autres chercheurs, ainsi qu'avec des créateurs de systèmes d'aide à la décision automatisée et fondés sur des données. Ils se sont également entretenus avec des fonctionnaires de police et d'autres responsables impliqués dans le fonctionnement de tels systèmes. En outre, ils ont mené des entretiens et échangé avec des personnes et groupes impactés par ces systèmes et par les mesures influencées par cesdits systèmes et mises en œuvre par la police et le système judiciaire pénal. Ils ont également interrogé différentes personnes travaillant avec ces groupes.
- ***Liberté d'information :*** les chercheurs ont exercé leur droit en vertu des lois en vigueur en matière de liberté d'information pour soumettre des demandes d'informations à la police locale et nationale, aux ministères et aux services pénitentiaires et de probation.
- ***Recherche open-source :*** les chercheurs ont examiné une variété de document accessibles au public, y compris des contrats, des états financiers, des évaluations et des études internes, des études d'impact, des sites web et des brochures d'entreprise, ainsi que d'autres informations connexes.
- Étude de la littérature universitaire existante : les chercheurs ont étudié et analysé

des études et des rapports sur ces systèmes, en se concentrant sur les aspects techniques de leur développement, de leur entraînement et de leur fonctionnement.

Questions de transparence

Il ressort clairement, à la lumière de toutes les études menées dans les différents pays, que les autorités policières et judiciaires cherchent à limiter et restreindre la divulgation ou la publication d'informations concernant les systèmes « prédictifs », de profilage et d'évaluation des risques.

Dans tous les pays, les demandes officielles adressées par les chercheurs aux ministères, aux services de police et aux autorités locales ont été refusées ou ignorées, souvent pour des raisons de secret commercial ou de sécurité nationale.[47] Les rares réponses fournies par les ministères concernés étaient en général vagues.[48] Les entreprises privées fournissent quant à elles des infrastructures et des outils opérationnels importants à la police. Elles ne sont toutefois pas soumises aux dispositions légales relatives à la liberté d'information.[49]

De même, la plupart des demandes d'entretien ont été refusées ou ignorées. En Espagne, ***AlgoRace*** a contacté plusieurs ministères pour solliciter des entretiens. Les personnes contactées avaient consenti à des entretiens individuels, mais les demandes ont malgré tout été refusées.

Compte tenu des enjeux techniques, juridiques et politiques importants qu'ils soulèvent, le manque de transparence concernant ces systèmes est inacceptable.

Systèmes « prédictifs » fondés sur une approche géographique

Les méthodes de police « prédictive » fondées sur une approche géographique sont développées pour déterminer où, et souvent quand, des crimes seront perpétrés afin d'allouer des ressources policières aux endroits appropriés. Les partenaires de recherche ont trouvé des exemples d'algorithmes prédictifs de la criminalité fondés sur une approche géographique dans chacun des pays étudiés : la Belgique, la France, l'Allemagne et l'Espagne.

Les défenseurs des systèmes de police « prédictive » fondés sur une approche géographique soutiennent que les méthodes axées sur les données peuvent optimiser la gestion policière. Selon eux, le fait d'identifier les zones à haut risque constitue une stratégie de prévention du crime efficace pour la police. Voici un résumé de cette approche :

> *« En concentrant ses ressources sur les individus et les endroits considérés à haut risque, ainsi qu'aux moments où des crimes sont susceptibles de se produire, la police parviendra à réduire plus efficacement la criminalité sur son territoire ».*[50]

En Europe, les chercheurs ont pu identifier deux types principaux de systèmes fondés sur une approche géographique :

— les algorithmes de prédiction des zones de criminalité potentielle ou « points chauds », qui s'appuient sur les données historiques des services de police afin

d’anticiper les futurs lieux de criminalité ;

— les algorithmes de prédiction des « risques » qui reposent sur l’hypothèse selon laquelle les facteurs environnementaux déterminent les endroits où les crimes sont commis.

Ces deux approches suscitent des préoccupations en termes de ciblage et de criminalisation disproportionnés des minorités raciales et des personnes et communautés à faible revenu.

Les exemples présentés dans ce rapport montrent que la police prédictive basée sur une approche géographique peut avoir de graves conséquences pour les personnes qui résident et travaillent dans des zones considérées comme « à haut risque ». Ces individus peuvent faire l’objet d’une surveillance policière plus stricte, de contrôles de véhicules et d’identité, de fouilles, d’interrogatoires ou même d’arrestations.

Bien que la Loi sur l’IA de l’UE interdise certains systèmes de police « prédictive » en vertu des directives officielles, la Loi ne s’applique toutefois pas aux systèmes « prédictifs » fondés sur une approche géographique.[51] La recherche met en évidence le potentiel de discrimination et de profilage de ces systèmes dont l’utilisation à des fins de police prédictive doit être interdite.

Le présent rapport ne donne qu’un aperçu des systèmes prédictifs de la criminalité fondés sur une approche géographique utilisés par les forces de police en Europe. Outre les systèmes utilisés en France, en Belgique, en Allemagne et en Espagne, selon des études précédentes, on trouve aussi des exemples similaires en Italie, en Suisse et au Royaume-Uni.

Prédiction des « points chauds » de la criminalité

En Belgique, en France, en Allemagne et en Espagne, les systèmes fondés sur une approche géographique utilisent principalement des méthodes de prédiction des « points chauds » de la criminalité. Ces méthodes permettent d’exploiter des données historiques sur la criminalité qui révèlent où et quand des faits de délinquance ont été commis et sont ainsi utilisées pour « prédire » les futurs lieux ou « points chauds » de la criminalité.

Les chercheurs ont identifié au moins neuf systèmes différents de prédiction des « points chauds ». Plusieurs ont déjà été déployés par des services de police de chaque pays.

En Allemagne :

— La police berlinoise a mis en œuvre un outil de classification des « lieux exposés à la criminalité » (*kriminalitätsbelastete Orte, kbO)* où des pouvoirs de police élargis peuvent être déployés ;[52]

— trois États fédéraux allemands ont adopté des systèmes de prédiction des « points chauds » de la criminalité, en baisse par rapport aux six États qui utilisaient cinq systèmes différents en 2018.[53] Parmi les systèmes utilisés citons :

- SKALA (*System zur Kriminalitätsauswertung und Lageantizipation*, Système d'analyse de la criminalité et d'anticipation des situations) en Rhénanie-du-Nord-Westphalie ;
- KrimPro (*Kriminalitätsprognose Wohnraumeinbruch*, Système de prévision des cambriolages résidentiels) à Berlin ;
- KLB-operativ (*Kriminalitätslagebild*, Situation de la criminalité) à Hesse ;[54] and

— La police bavaroise a utilisé le système de surveillance préventive de la criminalité (Pre-Crime Observation System, PRECOBS).[55]

Les systèmes « prédictifs » fondés sur une approche géographique sont largement utilisés en Espagne :

— le Système prédictif d'aide à la décision en matière de répartition des patrouilles (Predictive Police Patrolling Decision Support System, P3-DSS) est utilisé à l'échelle nationale ;[56]

— sept régions différentes utilisent un système EuroCop, dont la quasi-totalité des services de police de Madrid.[57]

Les chercheurs ont trouvé peu d'exemples d'applications actives de méthodes de maintien de l'ordre axées sur les « points chauds » en France et en Belgique. En France, ***La Quadrature du Net*** a identifié « PredVol » et PAVED, deux systèmes qui étaient utilisés par la ***Gendarmerie nationale,*** mais qui ont aujourd'hui été abandonnés.[58]

En Belgique, ***TechnoPolice*** a identifié un essai à petite échelle réalisé par la police de Westkust et l'utilisation du Système d'information géographique développé par la société Orbit, en Flandre et à Bruxelles.[59] Orbit affirme que son logiciel « a déjà été déployé dans près de 100 zones surveillées par la police ».[60]

À la suite d'un examen détaillé du système PredPol aux États-Unis, les systèmes de prédiction des « points chauds » de la criminalité ont suscité de vives critiques au niveau international dans la mesure où ils renforcent et perpétuent les biais raciaux.[61]

Les systèmes mentionnés dans ce rapport, y compris ceux qui emploient des techniques semblables à celles de PredPol, soulèvent également des inquiétudes en matière de discrimination et de criminalisation. Dans les quatre pays, les zones classées comme « à haut risque » par les systèmes de prédiction des « points chauds » de la criminalité correspondent souvent à des quartiers marginalisés où les habitants vivent et travaillent.

Finalités

Selon les autorités policières, les analyses statistiques permettant de prédire les « points chauds » de la criminalité contribuent à réduire les taux de criminalité. Florian Gauthier, expert en données français et créateur du système PredVol, justifie la nécessité de développer un modèle de prédiction des vols de véhicules dans les « points chauds » qui montrerait les écarts entre les zones patrouillées par les forces de l'ordre et les endroits touchés par les vols de véhicules. Selon lui, ces écarts peuvent être réduits grâce à l'utilisation des données relatives aux infractions pour orienter les patrouilles de police.[62]

Les méthodes « basées sur des preuves » permettraient de déployer des agents au bon endroit et au bon moment, ce qui aurait pour but de dissuader les activités criminelles. À Berlin, la police affirme que la désignation d'une zone comme « kbO » renforce le « sentiment de sécurité » et permet aux forces de l'ordre « de contrôler l'identité des personnes concernées, d'augmenter la détection et donc de prévenir les infractions pénales ».[63]

Plusieurs systèmes de police prédictive axés sur les « points chauds » identifiés concernent les vols ou cambriolages présumés :

— en France, PredVol est utilisé pour les vols présumés de voitures et PAVED [64] pour les vols de voitures et les cambriolages ;

— en Allemagne, le système PRECOBS cible les vols de véhicules et les cambriolages présumés. Le système KbO, quant à lui, s'intéresse principalement aux vols, ainsi qu'à d'autres infractions.[65] Des chercheurs ont émis l'hypothèse que les systèmes de prévision des « points chauds » pour les cambriolages auraient été mis en place vers 2010 suite à une couverture médiatique alarmiste sur les cambriolages ;[66]

— en Belgique, le système « prédictif » utilisé par la police locale de Westkust se concentre sur les cambriolages et les vols de véhicules ;[67]

— en Espagne, le système EuroCop est utilisé pour « prédire » les vols, parmi d'autres délits.[68]

Données utilisées

Les systèmes de prédiction des « points chauds » de la criminalité utilisent des analyses statistiques et des tendances tirées d'importants volumes de données sur la criminalité, souvent issues des bases de données de la police, afin de prédire où les crimes sont susceptibles de se produire à l'avenir.

En Allemagne, le modèle prédictif de la criminalité basé sur une approche géographique kbO (***Kriminalitätsbelastete Orte*** ou Lieux exposés à la criminalité) utilise une

évaluation statistique qui intègre des données sur la criminalité et d'autres informations supplémentaires non spécifiées.[69]

En Belgique, le Système d'information géographique Orbit, qui semble être utilisé par plus de 100 services de police municipaux, s'appuie sur des données criminelles historiques de la police pour déterminer les futurs « points chauds ».[70] The Westkust local police force system Le système utilisé par la police locale de Westkust exploite de la même manière les données des services de police sur les délits présumés, les plaques d'immatriculation, les dossiers judiciaires et même les conditions météorologiques.[71]

En France, le système PredVol s'appuie sur des données relatives aux vols de voitures provenant des systèmes informatiques utilisés pour enregistrer les plaintes et signalements, notamment :

- les coordonnées XY de l'endroit où le vol de voiture a eu lieu ;
- la date ;
- toute information complémentaire sur le modèle et la couleur du véhicule.[72]

En Espagne, le système EuroCop est capable d'exploiter et d'intégrer plusieurs sources d'information, notamment les données et les fichiers de la police sur la criminalité, les données socio-économiques, ainsi que les données de vidéosurveillance. Ces informations sont compilées dans un modèle algorithmique destiné à « prédire » la criminalité et générer des « cartes thermiques » et des « itinéraires de patrouille » pour les services de police.[73]

L'utilisation des données historiques des services de police dans les systèmes de prédiction des « points chauds » de la criminalité soulève des craintes légitimes en matière de discrimination illégale. Comme nous le verrons plus loin, les données historiques sur la criminalité indiquent une présence policière excessive et une criminalisation des communautés précarisées et exposées au racisme. Les algorithmes des « points chauds » de la criminalité intègrent cette disproportion et cette discrimination dans les prédictions futures.

En effet, le ministre de l'Intérieur belge a lui-même admis en juin 2020 : « Les données statistiques de la police ne représentent pas la criminalité dans une zone donnée, mais reflètent plutôt l'activité de la police en elle-même. »[74]

Plusieurs systèmes de prédiction des « points chauds » utilisent également des

données socio-démographiques dans les ensembles de données d'entraînement. Le développeur de PredVol a déclaré à ***La Quadrature du Net*** que le système utilisait 600 variables socio-démographiques. Parmi celles-ci figurent la fréquentation scolaire et le taux de chômage, le nombre de commerces à proximité et l'âge moyen de la population. Les autorités n'ont pas fourni d'informations plus complètes.[75] En outre, ils ont également constaté que, parmi 15 variables socio-démographiques, PAVED se nourrissait notamment de données relatives au genre, à la citoyenneté, à l'immigration, au revenu du ménage et au niveau d'éducation.[76]

Le système de « patrouille intelligente » P3DSS de la police nationale espagnole utilisait lui aussi des données axées sur la nationalité, répartissant les habitants de Madrid en différents groupes, à savoir : les citoyens espagnols, les autres citoyens de l'UE, les citoyens non européens et les citoyens par continent, un groupe que l'on ne retrouve pas souvent.[77] Le système calculait ensuite pour chaque groupe de nationalité un « objectif de contact policier », soit le temps de patrouille alloué à chaque groupe en fonction de sa taille par rapport au territoire géographique.[78] Bien qu'extrêmement généralisés, ces groupes démographiques sont en réalité des substituts de groupes raciaux.

Les données relatives à la nationalité, au statut d'immigrant et au genre sont, ou peuvent être considérées, comme des « catégories particulières » de données.[79] Entre autres facteurs, ces variables socio-démographiques pourraient établir un lien entre la criminalité, la race et le dénuement économique. La législation européenne en matière de protection des données stipule clairement que :

> *« Tout profilage qui entraîne une discrimination à l'égard de personnes physiques sur la base de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, devrait être interdit ».*[80]

À partir de ces données d'entrée, les systèmes de prédiction des « points chauds » ont recours aux analyses statistiques pour déterminer la probabilité des futurs lieux de criminalité. Les méthodes de modélisation particulières nécessaires pour effectuer ces analyses géographiques et temporelles varient considérablement selon les différents systèmes.

Les systèmes PAVED et PredVol utilisent des techniques d'apprentissage automatique qui leur permettent d'apprendre automatiquement à partir de données additionnelles, sans qu'il soit nécessaire de les entraîner manuellement. La plupart des autres systèmes de prédiction des « points chauds » identifiés en Belgique, en France, en Allemagne et en Espagne se basent sur des algorithmes.

Résultats

En règle générale, ces systèmes de prédiction des « points chauds » permettent aux services de police d'obtenir une « carte thermique » des zones ou lieux susceptibles

de présenter un taux élevé de criminalité. En Allemagne par exemple, l'outil PRECOBS affiche une carte avec des zones marquées de différentes couleurs. Ces couleurs représentent la probabilité supposée, ou les niveaux de risque, qu'un crime se produise dans cette zone (voir Figure 1).

FIGURE 1 : CAPTURE D'ÉCRAN PRECOBS DU CODE COULEUR DE LA CARTOGRAPHIE D'UN LIEU. RÉFÉRENCE PHOTO : SONJA PETERANDERL

Les officiers de police peuvent accéder à certains systèmes, comme PredVol en France, « sur le terrain » via leurs tablettes. D'autres systèmes, comme PAVED, ne sont accessibles qu'aux commandants. Outre les « cartes thermiques », PAVED propose également des histogrammes affichant les variables socio-démographiques considérées comme des indicateurs de criminalité particulièrement pertinents (voir Figure 2).

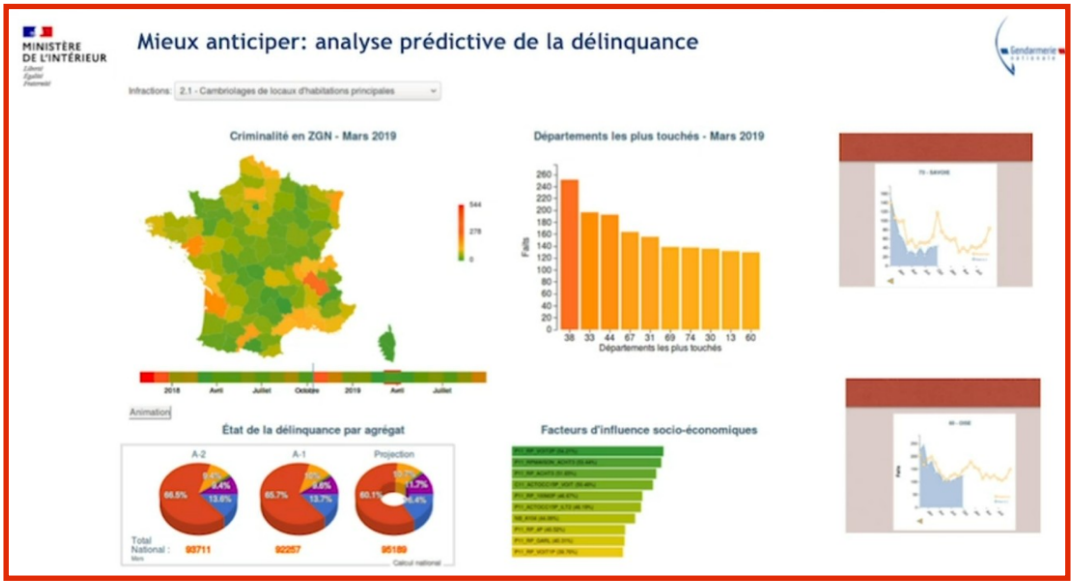


FIGURE 2 : CAPTURE D'ÉCRAN DE LA CONFÉRENCE DONNÉE PAR LE COLONEL PATRICK PERROT, COLLOQUE DE L'INSTITUT DE DROIT PRIVÉ - UT CAPITOLE - 8 SEPTEMBRE 2021 (SOURCE : « AI ET ENJEUX DE SÉCURITÉ » À 23 MIN 10 S).

Les systèmes de prédiction des « points chauds » de la criminalité permettent d'allouer des ressources policières et de déterminer où et quand patrouiller au niveau des zones identifiées. Parmi les mesures mises en place dans les « points chauds », on peut citer :

— la surveillance ;

— la collecte d'informations ;

— les contrôles d'identité ;

— les interrogatoires ;

— les fouilles ;

— les ordonnances de protection ;

— les arrestations.[81]

Lorsqu'une zone est désignée comme « point chaud », des pouvoirs de police élargis peuvent y être déployés. À Berlin, la police est autorisée par la loi à procéder à des contrôles d'identité ou à des fouilles visant des personnes ou des objets dans des zones classifiées « kbO », en l'absence de soupçons concrets, mais en se basant plutôt « sur le comportement ».[82]

De même, ***La Quadrature du Net*** s'est entretenue avec une source qui a indiqué que les « points chauds » générés par PAVED étaient utilisés pour obtenir des autorisations spéciales auprès des procureurs afin de procéder à des contrôles d'identité et de véhicules dans ces lieux. La police administrative pouvait ainsi utiliser des pouvoirs de police judiciaire, un manquement majeur aux obligations de police administrative.[83]

Impacts

Les lieux désignés comme « points chauds » de la criminalité par les systèmes algorithmiques représentent de manière disproportionnée des quartiers où vivent et travaillent des communautés précarisées et exposées au racisme. L'experte juridique Lina Schmid indique que les endroits classés « kbO » comptent en grande partie une population majoritairement perçue comme étant composée de migrants.[84]

Suite à la mise en place du système PRECOBS en Bavière, Matthias Monroy, rédacteur en chef de la revue allemande sur les droits civils ***Bürgerrechte & Polizei*** (***Droit civil et maintien de l'ordre***) a déclaré :

> *« Qui la police arrête-t-elle le plus souvent lorsqu'elle soupçonne qu'un cambriolage risque de se produire dans les heures ou les jours à venir ? Je dirais qu'il s'agit plutôt de personnes mal habillées, de personnes ayant une couleur de peau différente ou portant des sweats à capuche ; il s'agit-là de stéréotypes qui existent déjà au sein de la police ».*[85]

La Constitution allemande interdit les contrôles effectués par la police sur la base de critères raciaux (article 3 de la ***Grundgesetz*** ou Loi fondamentale). Toutefois, Lina Schmid explique que le fait de désigner certaines zones comme « points chauds » de la criminalité permet à la police de contourner cette interdiction :

> *« Ce sont des quartiers entiers. ainsi que les personnes qui les fréquentent. qui sont criminalisés et non pas des individus issus d'un groupe racial, comme c'est souvent le cas dans le cadre du profilage racial. Par conséquent, la police a la possibilité de pratiquer le profilage racial en toute opacité, car même si toute la population est censée faire l'objet d'un contrôle. dans la pratique, ce sont surtout les personnes noires, indigènes et de couleur qui sont ciblées par la police. »*[86]

Wrangelkiez United, une initiative des habitants, a indiqué que les contrôles ciblant Görlitzer Park/Wrangelkiez classés kbO touchent presque exclusivement les personnes noires et les minorités raciales, « indépendamment de leur activité ou des endroits qu'elles fréquentent ».[87] Les élèves d'une école de langues du quartier sont contrôlés sur le chemin des cours et les hommes noirs font régulièrement l'objet de contrôles dans le parc, comme l'indiquent des témoignages vidéo recueillis par ***Wrangelkiez United*** :

> *« Lorsque la police est présente (...), les personnes de couleur, comme moi, sont contrôlées sans véritable raison, et ce n'est pas parce que nous avons commis des infractions. C'est à cause de notre apparence ».*[88]

Prédiction des risques

En Europe, les systèmes fondés sur une approche géographique comprennent également des systèmes de prédiction des risques qui s'appuient sur des données environnementales ou contextuelles pour identifier les lieux supposés plus propices à la criminalité.

Ces systèmes de prédiction des risques basés sur l'environnement s'appuient sur la théorie des « vitres brisées » appliquée en criminologie. Cette théorie soutient que l'environnement physique est un facteur déterminant de la criminalité. Elle a été développée par James Wilson et George Kelling aux États-Unis en 1982.[89] Cette théorie se base sur l'hypothèse selon laquelle certains facteurs environnementaux, comme les vitres brisées, peuvent servir d'indicateurs ou d'éléments dissuasifs de la criminalité.

La théorie des « vitres brisées » a ensuite été déployée et appliquée à l'échelle des services de police aux États-Unis. Un exemple fréquemment évoqué est celui des modifications apportées par l'ancien chef de la police de New York, William Bratton.[90] Cette théorie a depuis inspiré la création et le développement de méthodes de maintien de l'ordre fondées sur des données. Toutefois, elle a été largement discréditée par plusieurs criminologues et sociologues.[91]

Tout comme les algorithmes des « points chauds » de la criminalité, les algorithmes de « risques » liés à l'environnement peuvent orienter la police vers des secteurs urbains économiquement défavorisés, la plupart du temps fréquentés ou habités par des communautés exposées au racisme.

Finalités

Les forces de police belges et françaises utilisent le RTM ou Risk Terrain Modelling, un modèle algorithmique qui sert à prédire la criminalité ou la délinquance et qui tient compte de l'évaluation du « risque » environnemental. Le RTM est également utilisé par la police britannique.[92]

La méthodologie RTM a été développée par Joel Caplan et Leslie Kennedy, deux universitaires de l'université Rutgers dans le New Jersey aux États-Unis. Le RTM aurait été testé dans plus de 45 pays sur six continents. Le site Web du Risk Terrain Modelling, qui fait la publicité du logiciel développé par la société Simsi, indique ce qui suit :

> *« Le RTM permet d'identifier les risques liés aux caractéristiques d'un environnement et de modéliser la façon dont ces caractéristiques coexistent pour créer un cadre des comportements uniques propices à la criminalité.*
>
> *Lorsqu'on pense aux endroits propices aux activités criminelles, on s'imagine presque toujours une rue déserte et sombre. Dans ce cas de figure, on*

tient compte d'au moins deux caractéristiques environnementales : (1) une rue et (2) un éclairage inadéquat. On estime donc que le risque de criminalité est exceptionnellement élevé dans les endroits où ces caractéristiques particulières coexistent ».[93]

Le site web fait la distinction entre le RTM et les méthodes de prédiction des « points chauds » de la criminalité :

« Les points chauds révèlent les foyers de criminalité, sans préciser les raisons sous-jacentes. On se concentre trop souvent sur les points chauds sans tenir compte des aspects spatiaux qui font de ces zones des lieux propices à la délinquance. Les points chauds ne révèlent que les signes et les symptômes des endroits propices à la criminalité. Le RTM permet d'aller plus loin en fournissant un diagnostic spatial. »[94]

Le RTM est actuellement utilisé dans la vallée de la Senne (Belgique) et à Paris (France). La ***Direction de la Sécurité de Proximité de l'Agglomération Parisienne*** (DSPAP) avait décidé d'utiliser l'algorithme après qu'un géo-statisticien de l'ancien ***Observatoire National de la Délinquance et des Réponses Pénales*** (ONDRP)[95] ayant travaillé pendant plusieurs années avec l'Université de Rutgers a déclaré :

« J'utilise l'algorithme RTM (Risk Terrain Modeling) depuis plus de huit ans. [...] Aujourd'hui, c'est une appli web, beaucoup plus puissante qu'avant, mais c'est le même principe : cela rejoint la prévention situationnelle, c'est-à-dire qu'on repère les éléments contextuels, environnementaux qui font que ça se passe là. [...] Donc en analysant un contexte, en identifiant les facteurs qui aggravent le risque, on peut prévoir pour un environnement similaire ce qui peut éventuellement se produire. »[96]

Dans la vallée de la Senne, il est utilisé à des fins similaires. Le programme a été piloté par Anneleen Rummens, doctorante à l'université de Gand, sous la supervision du professeur de criminologie Wim Hardyns.[97]

Il existe d'autres systèmes de prédiction des risques basés sur l'environnement qui n'utilisent pas l'algorithme RTM. Il s'agit notamment de MapRevelation et du « module prédictif » du système Smart Police utilisé en France. MapRevelation a été l'un des premiers systèmes de police « prédictive » à être déployé en France. Commercialisé par la société Sûreté Globale,[98] il est utilisé par les autorités locales et les forces de police municipale de Montpellier, Lyon, Lille, Villeurbanne, Montauban, Angers, Colombes et Melun Val de Seine.[99]

Données utilisées

Le système RTM s'appuie sur différents « facteurs de pondération » qui sont intégrés au modèle final. Ces facteurs peuvent être ajustés en fonction du cas d'utilisation spécifique du modèle. L'algorithme attribue une valeur de vulnérabilité aux lieux en fonction de facteurs spatiaux, tels que :

— l'éclairage public ;

— les arrêts de bus ou de métro ;

— les terrasses de cafés ;

— les fast-foods ;

— les toilettes publiques ;

— les pharmacies ;

— les épiceries ;

— les bars ;

— la présence d'arbres ou de bancs ;

— certains types de magasins ;

— les écoles ;

— les bureaux de poste.

Sur le site Web du Risk Terrain Modelling, d'autres exemples de facteurs sont proposés, notamment les suivants : « drogues », « inoccupés » et « gangs ».[100]

À Paris, le système RTM s'appuie sur les données du ***Logiciel de Rédaction des Procédures de la Police Nationale*** (LRPPN). Il permet d'établir des corrélations entre les actes de délinquance et les facteurs dits environnementaux. En 2018, Jean-Luc Besson, chef du département géostatistique de l'ONDRP, a apporté plus de précisions sur les facteurs susceptibles d'être utilisés dans le modèle parisien :

> *« Si on prend les vols à la tire près des distributeurs, on va se demander : les plus concernés sont-ils ouverts le jour et la nuit ? Sont-ils situés à proximité d'un*

carrefour, d'une gare, etc. ? ».[101]

Les chercheurs n'ont pas pu obtenir d'informations précises sur toutes les variables utilisées dans les systèmes RTM déployés à Paris et dans la vallée de la Senne. Toutefois, on sait que le modèle de la vallée de la Senne se base sur des facteurs tels que les conditions météorologiques pour des événements spécifiques.[102]

En France, MapRevelation aurait été entraîné sur une base de données du « terrorisme », dans le but de « prédire » des attentats.[103] L'outil est également alimenté par des données détenues par les forces de police municipales qui utilisent le système.

Le « module prédictif » Smart Police, développé par la société française Edicia, utilise des techniques d'apprentissage automatique. Il s'appuie à la fois sur les données opérationnelles de la police (p. ex. procès-verbaux, infractions, localisation des agents et des véhicules) et sur des données urbaines (p. ex. données environnementales et météorologiques, événements nationaux et locaux, données socio-démographiques et électorales).

Le module « prédictif » Smart Police exploiterait également des informations provenant des réseaux sociaux et d'autres sources, comme par exemple des directeurs de collèges et lycées et des propriétaires de logements sociaux, ainsi que des informations de première main fournies par des officiers de police.[104] Cette approche présente le risque évident d'encoder des rumeurs, ouï-dire et opinions non vérifiées dans des systèmes algorithmiques, sous couvert d'objectivité technique.

Résultats

La culture du secret au sein des forces de police et des organismes gouvernementaux a compliqué la recherche d'informations concrètes sur les résultats produits par les systèmes de prédiction des « risques » liés à l'environnement utilisés en Belgique et en France.

Selon une source contactée par ***La Quadrature du Net***, il n'existe aucune preuve concluante que le système RTM réduit les taux de criminalité en France. La source a également indiqué que la méthodologie RTM n'incite pas les institutions qui l'utilisent à réfléchir aux causes structurelles de la criminalité.[105] On retrouve le même problème avec d'autres systèmes de prédiction des « points chauds » de la criminalité.

Autres systèmes de « prédiction » de la criminalité fondés sur une approche géographique utilisés en Europe

Outre les systèmes décrits ci-dessus déployés en Belgique, en France, en Allemagne et en Espagne, d'autres forces de police en Europe utilisent également des systèmes de

police « prédictive » fondés sur une approche géographique.

Au Royaume-Uni, ***Amnesty International UK*** a récemment constaté que près des trois quarts des services de police utilisaient des systèmes de police « prédictive », dont 32 sur 46 ont recours à des systèmes de « prédiction » de la criminalité fondés sur une approche géographique.[106] ***Amnesty*** a enquêté sur l'usage du RTM par les forces de police britanniques et a observé que l'utilisation de ce système par la police métropolitaine de Londres « contribue et renforce le profilage racial et le maintien de l'ordre favorisant la discrimination ».[107] Les analyses démographiques des zones qualifiées « à haut risque » par l'algorithme RTM ont montré que :

> *« ... les zones où le système RTM anticipe des actes violents graves correspondent de manière significative à des quartiers à forte densité de populations défavorisées, notamment d'origine africaine, caribéenne, bangladaise ou pakistanaise ».*[108]

Le Dr Adam Elliott-Cooper, universitaire et auteur de ***Black Resistance to British Policing***, a déclaré à propos de l'utilisation de facteurs de « risque » liés à l'environnement visant à « prédire » la criminalité :

> *« C'est sans surprise que le type d'environnement ciblé par la police ne correspond pas à des maisons mitoyennes séparées par des clôtures blanches. Les environnements ciblés sont des cités en milieu urbain avec une forte présence policière et non pas les banlieues riches. Nous verrons donc comment cette approche prétendument axée sur la géographie et donc prétendument plus scientifique et objective du maintien de l'ordre ne fait en fait que reproduire ces problèmes existants ».*[109]

Aux Pays-Bas, la police utilise le « Système d'anticipation de la criminalité ». Ce système de prédiction des « points chauds » s'appuyait à l'origine sur des points de données comme le nombre de personnes d'origine « non occidentale » ayant au moins un parent né à l'étranger et vivant dans une zone en particulier. Bien que ces points de données aient été supprimés par la suite, le système a continué d'utiliser des données historiques sur la criminalité, ainsi que des variables de substitution pour la race et la classe, telles que les données sur les revenus et les prestations sociales.[110]

Il y a quelques années, la police italienne utilisait « Delia », un système développé par la société KeyCrime. Ce système était doté de fonctions de « prédiction » de la criminalité axées sur les individus et la géographie. Il s'agirait de l'un des premiers exemples au monde de logiciel de police « prédictive » commercialisé et mis en service dès 2008.[111] Cependant, KeyCrime a depuis été placé en liquidation judiciaire en raison de l'incertitude financière causée par l'adoption de Loi sur l'IA de l'UE et du risque de voir son système devenir illégal.[112]

Le système XLAW continue cependant d'être utilisé en Italie.[113] XLAW est un outil de prédiction des « risques » basés sur l'environnement, similaire aux systèmes RTM utilisés en France, en Belgique et au Royaume-Uni. Parmi les prédicteurs spatio-temporels du système figurent : les grandes manifestations, les pensions de retraite reçues en fin de mois, les heures de fermeture des magasins, les arrivées de trains et de bateaux et les variations météorologiques.[114]

Dans certains cantons suisses, la police utilise le système PRECOBS, également utilisé en Allemagne.[115]

Systèmes de profilage et de « prédiction » de la criminalité axés sur la personne

Les outils de « prédiction » de la criminalité axés sur la personne visent à évaluer la probabilité ou le « risque » qu'une personne commette certaines actions, en particulier celles définies par la loi comme étant des infractions pénales. Plutôt que de se focaliser sur un lieu particulier, ils visent des individus spécifiques.

Les autorités policières et judiciaires pénales utilisent ces systèmes pour tenter de profiler, de « prédire » ou d'évaluer le « risque » qu'une personne commette une infraction pénale ou se livre à des actes criminels. D'autres systèmes de ce type tentent de déterminer la probabilité qu'une personne puisse être victime d'un crime, comme la violence basée sur le genre. Ils ont également été utilisés pour tenter de détecter les faux signalements de crimes.

Les personnes ciblées par ces systèmes font l'objet d'une évaluation de leurs informations personnelles, de leurs antécédents, de leur situation actuelle, ainsi que de leur réseau familial et social. Le but est de comprendre et d'anticiper le comportement, le niveau de dangerosité ou la délinquance présumée de ces personnes, ce qui peut entraîner des conséquences potentiellement graves. Ces systèmes pourraient mener à la mise sous surveillance de certains individus qui risquent de subir davantage de contrôles policiers, d'interrogatoires, de fouilles, de visites à leur domicile ou sur leur lieu de travail. Le

recours à ces systèmes peut même conduire à la détention, à l'arrestation ou à l'expulsion des personnes visées.

Ces outils sont également utilisés dans le système juridique pénal. Ils peuvent influencer la prise de décision des juges, y compris la détermination de la peine, ainsi que la durée d'emprisonnement d'une personne, la date de sa libération et les conditions de sa détention.

Finalité

Les systèmes « prédictifs », de profilage et d'évaluation des risques axés sur la personne sont utilisés à des fins très diverses. Certains services utilisent des logiciels d'exploration et d'analyse de données pour collecter et compiler des données, évaluer les tendances et les utiliser pour « prédire » des modèles futurs.

En Allemagne, trois États fédéraux détiennent des licences d'exploitation de programmes d'exploration et d'analyse de « big data » basés sur le logiciel Gotham développé par l'entreprise technologique américaine Palantir. Comme beaucoup d'autres entreprises qui développent et vendent des solutions technologiques pour la police, la société Palantir est très discrète concernant la technologie développée et les contrats signés.

La police de l'État de Hesse, en Allemagne, se sert de ***hessenDATA***, un système géré par Palantir conçu pour créer des profils complets d'individus. Le système peut fournir des informations détaillées sur une personne, notamment la date et l'endroit des interpellations, les arrestations éventuelles, les contrôles de stupéfiants et l'adresse du domicile.

En Belgique, le système « i-Police » utilisé par la police nationale belge dispose de multiples fonctions, notamment :

— l'analyse et la « prédiction » de tendances ;

— la prédiction de la criminalité future à des fins de « prévention » ;

— le contrôle et la surveillance ;

— l'organisation des patrouilles de police, des contrôles et des vérifications ;

— et d'autres formes d'intervention et de contrôle.[116]

La police belge procède également au profilage de personnes et de groupes et gère des bases de données spécifiques à cette fin, ce que nous examinerons plus en détail ci-dessous. Ces bases de données sont notamment utilisées pour cibler les « gangs urbains », un terme chargé de racisme.[117] Les personnes profilées car soupçonnées d'être membres de « gangs » ont subis des contrôles et des fouilles et ont fait l'objet de surveillances et d'interpellations.[118]

Des outils de « prédiction » de la criminalité, de profilage et d'évaluation du

« risque » ciblant des individus ont été déployés en Allemagne pour évaluer le risque futur supposé posé par des soi-disant terroristes islamistes[119] ou partisans du terrorisme. L'Office fédéral de la police criminelle a mis au point deux systèmes d'évaluation du risque ciblant des individus appelés RADAR (Analyse basée sur des règles pour l'évaluation du risque accru avec potentiel de destruction posé par des délinquants).

RADAR-iTE, une itération de ce système, est un outil utilisé pour analyser et profiler les soi-disant « islamistes ». La police fédérale belge a également déclaré qu'elle utilisait un outil similaire à RADAR-iTE.[120] L'autre itération, RADAR-rechts, est utilisée par l'Office fédéral allemand de police criminelle afin de profiler les personnes ayant des opinions de droite et considérées comme violentes. Un autre outil, RADAR-Haft (« RADAR-détention »), est également en cours de développement. Il servira à évaluer la propension à la violence des personnes incarcérées à leur sortie de prison.

L'objectif des outils RADAR-iTE et RADAR-rechts est principalement d'évaluer le risque lié aux personnes préalablement identifiées comme « Gefährder » (dangereuses). Cette classification des menaces mise au point par les autorités chargées de l'application de la loi allemandes a été déployée dans toute l'UE.[121] La terminologie est vague et l'interprétation subjective. Ces systèmes sont également utilisés pour évaluer les « personnes concernées », une autre catégorie floue et sujette à interprétation. Le profilage du risque sert à évaluer et classer par ordre de priorité les individus « à haut risque » en vue de la mise en œuvre ultérieure de mesures répressives et d'interventions.[122]

En Espagne, VioGén est l'un des systèmes d'évaluation du risque parmi les plus connus ciblant des individus. Son objectif est d'évaluer le risque de violence basée sur le genre pour une personne ayant signalé un incident. L'évaluation permet de déterminer les mesures que la police mettra en œuvre.[123]

En outre, les autorités espagnoles ont également mis en place un système « prédictif » plutôt insolite. VeriPol est un système algorithmique utilisé par la police nationale espagnole afin de détecter les faux signalements de crimes. Il utilise des méthodes de traitement automatique du langage pour examiner les textes des procès-verbaux concernant les cambriolages, les vols à la tire et les vols de sacs à main. Il est aussi utilisé comme détecteur de mensonges. Cette technologie a été développée pour combattre la fraude liée aux faux signalements. Son objectif principal est de fournir aux agents une évaluation rapide pour déterminer si un signalement est potentiellement frauduleux.[124] En mars 2025, la police nationale espagnole a mis fin à l'utilisation de VeriPol. Le ministère de l'Intérieur espagnol a déclaré que cette décision était due au fait que le système ne pouvait être utilisé dans le cadre de procédures judiciaires.[125]

Dans le monde entier, y compris en Europe, les autorités chargées de la sécurité analysent de plus en plus les dossiers passagers (Passenger name record, PNR). Il

s'agit de données à caractère personnel collectées par les compagnies aériennes à des fins commerciales lorsqu'une personne réserve un vol.[126] Ces données PNR sont recoupées avec celles de la police et d'autres bases de données nationales. Des algorithmes sont utilisés pour détecter systématiquement des tendances dans ces données en fonction de critères prédéterminés.[127] De tels systèmes renversent la présomption d'innocence et font de toute personne voyageant par avion un suspect.[128] L'UE envisage d'étendre le recours à ce type de système à d'autres formes de transport, à commencer par le transport maritime.[129]

Les prisons espagnoles utilisent le système DRAVY pour tenter d'identifier les détenus soupçonnés de radicalisation « djihadiste ».[130] L'objectif principal de DRAVY est d'évaluer le niveau de radicalisation « djihadiste ». Il est par conséquent fondamentalement discriminatoire dans la mesure où il cible presque exclusivement les musulmans et les personnes d'origine musulmane. Le système a été conçu pour cibler le « djihadisme », un terme qui repose lui-même sur des stéréotypes occidentaux discriminatoires.

RisCanvi est un outil similaire qui est également utilisé dans les prisons espagnoles pour « prédire » le risque de récidive. Il aide à la décision en matière de libération conditionnelle, de libération provisoire et de catégorisation des prisonniers.[131]

Données utilisées

Ces systèmes sont entraînés, développés et exploités grâce à des données provenant de la police, des autorités chargées de l'application de la loi et du système judiciaire pénal.

Souvent, ces autorités collectent ou accèdent à des données provenant de nombreuses sources différentes. En Allemagne, les systèmes Palantir utilisent des données provenant de bases de données policières, ainsi que d'autres sources, y compris les réseaux sociaux. Ces dernières années, des recours en justice ont été introduits contre ces systèmes et contre les lois sur l'analyse des données qui sous-tendent leur utilisation.[132] Lorsqu'un recours en justice a abouti à une restriction de la portée des analyses et des sources de données, une source policière allemande a déclaré : « Lorsque la décision a été rendue, les collègues ont exprimé leur mécontentement car leur champ d'action a été restreint ».[133]

Le système belge i-Police a pour but d'intégrer des données provenant des séquences de vidéosurveillance et des bases de données de la police belge. Il utilise également des « renseignements » open-source, provenant notamment des réseaux sociaux et des rapports de presse. À cette fin, i-Police déploie des technologies numériques provenant de différents sous-traitants, dont un certain nombre d'entreprises israéliennes telles qu'Interionet et TA9/Rayzone. Le PDG de TA9/Rayzone avait occupé le poste de directeur adjoint de l'Unité 8200, l'unité de renseignement de l'armée israélienne responsable du développement et du déploiement de « Gospel », un système de ciblage assisté par l'IA utilisé pour automatiser le bombardement de Gaza dans le cadre du génocide et du massacre de

Palestiniens perpétrés par Israël.[134]

Les données utilisées par ces systèmes sont fondamentalement biaisées. Dans toute l'Europe, la police cible de manière disproportionnée les personnes issues de minorités ethniques. Par exemple, en Espagne, la police interpelle et fouille de manière disproportionnée les personnes en fonction de leur apparence raciale, ethnique ou religieuse.[135] En Allemagne, les ressortissants étrangers sont surreprésentés parmi les suspects fichés par la police, les individus condamnés par les tribunaux ou incarcérés.[136] Le système de justice pénale belge a été condamné à plusieurs reprises pour des faits racistes, notamment pour avoir recouru au profilage ethnique.[137] Le Comité des Nations unies pour l'élimination de la discrimination raciale (CERD) a exprimé ses inquiétudes concernant la surreprésentation des personnes d'origine étrangère dans le système de justice pénale belge, en particulier dans les prisons.[138]

Les données provenant des autorités policières et judiciaires pénales utilisées dans ces systèmes numériques comportent énormément de biais structurels et institutionnels, ainsi que des surreprésentations et des discriminations. Pourtant, ces mêmes données servent à développer et exploiter des systèmes « prédictifs », de profilage et d'évaluation des risques. Il en résulte un ciblage accru des mêmes groupes et communautés marginalisés. Les résultats de ces opérations sont ensuite réintégrés dans les systèmes. Cette méthode augmente la probabilité que les membres de ces groupes et communautés soient considérés comme présentant un risque élevé à l'avenir. Ces algorithmes produisent ainsi une prophétie auto-réalisatrice ou un risque d'auto-renforcement. Il existe des exemples clairs de la manière dont ces données discriminatoires influencent les résultats produits par ces systèmes.

On ne dispose pas de la liste complète des données utilisées par le système de profilage allemand RADAR-iTE. Ce système repose toutefois sur une évaluation distante sans contact direct avec la personne évaluée.[139] L'évaluation porte sur des sujets tels que « la violence contre autrui », « l'interaction avec les autorités et d'autres institutions » et « l'armée et les voyages ». D'autres questions sont également posées : « À quoi ressemble sa vie privée ? La personne est-elle plutôt solitaire ou évolue-t-elle au sein d'un groupe ? A-t-elle des contacts en dehors de la mouvance islamiste ? A-t-elle un travail ? ».[140]

Ces éléments de profilage ont pour conséquence que toute personne ayant voyagé depuis une zone de conflit, vers une destination touristique ou pour des motifs familiaux, peut être considérée comme suspecte ou « à risque ». Des points de données tels que les associés, les contacts ou les habitudes de voyage peuvent clairement conduire à la

discrimination.[141] L'évaluation RADAR-iTE contient également d'autres éléments préoccupants et potentiellement discriminatoires, notamment sur les problèmes de santé mentale et les tendances suicidaires.[142]

Des problèmes ont également été constatés en ce qui concerne les données utilisées pour entraîner le système espagnol VeriPol (aujourd'hui abandonné) qui servait à détecter les faux signalements de crimes. VeriPol a été entraîné sur la base de plaintes déposées à la police, puis classées manuellement par un agent comme étant fausses ou réelles. Cependant, il semble difficile de pouvoir se prononcer définitivement sur la véracité ou la fausseté des faits allégués si les plaintes ne sont pas toutes résolues. Le modèle a donc été entièrement développé à partir de suppositions émises par l'agent responsable du traitement des plaintes.[143] Compte tenu de ces problèmes, il est surprenant qu'il ait fallu attendre au moins sept ans avant que les autorités espagnoles ne décident de mettre fin à l'utilisation du système.

En Espagne, le système VioGén aurait été conçu pour déterminer la probabilité qu'une personne soit victime de violence basée sur le genre. Toutefois, le système utilisait non pas les témoignages des victimes de violence basée sur le genre, mais des procès-verbaux de plaintes déposées par des femmes. Le score de risque ainsi obtenu dépend donc entièrement de l'évaluation effectuée par l'officier de police.[144] En outre, le système ne peut traiter que des données provenant de plaintes effectivement déposées.

Cependant, de nombreux incidents de violence basée sur le genre ne sont pas signalés, en particulier ceux touchant les femmes migrantes, les femmes issues de milieux marginalisés et défavorisés et les mères de famille. Au même titre que les personnes LGBTQIA+ et les personnes en situation de handicap, ces groupes sont les plus touchés par les difficultés structurelles à dénoncer leurs agresseurs. Le système ne prend pas suffisamment en considération l'expérience des personnes les plus marginalisées au sein de la société.[145]

Les concepts qui sous-tendent ces systèmes « prédictifs », de profilage et d'évaluation des risques sont également fondamentalement biaisés. Ce problème découle d'un manque de clarté qui entraîne une subjectivité ou de l'utilisation de termes culturellement spécifiques avec des sous-entendus racistes.

En Allemagne, des termes vagues comme « Gefährder » (dangereux/se) et « relevante Person » (personnes d'intérêt) sont utilisés pour catégoriser les personnes soupçonnées de commettre ou de soutenir des actes de violence. Ces termes sont aujourd'hui couramment utilisés par les services de sécurité et les forces de police et ont été intégrés dans les systèmes RADAR. Ils sont vagues, peu scientifiques et n'ont pas été clairement définis juridiquement. Cela signifie que quiconque peut faire l'objet d'un profilage subjectif, de manière incohérente, à la discrétion des autorités, ce qui remet totalement en question la légitimité du système.

Ces problèmes sont mis en évidence par l'utilisation pratique de ces termes. Les forces de l'ordre allemandes se sont montrées beaucoup plus réticentes à considérer les extrémistes de droite comme une menace aussi dangereuse que les soi-disant « islamistes ». Par exemple, lorsque l'organisation terroriste néo-nazie NSU (National Socialist Underground) a été identifiée en 2011, seuls quatre de ses membres ont été classés comme « Gefährder ».[146]

Les données utilisées dans ces systèmes posent d'autres problèmes. Le système belge i-Police recueille des données provenant de multiples sources policières, y compris des informations « non validées ». Il s'agit notamment d'informations non corroborées provenant de procès-verbaux, souvent décrites comme des « renseignements » de police, par exemple des informations concernant des personnes qui n'ont pas été condamnées ou inculpées. Le président de l'autorité de protection des données qui supervise la police belge, le COC, a exprimé de sérieuses inquiétudes quant à l'utilisation de ces données dans le système i-Police.[147]

Les systèmes d'évaluation de la criminalité potentielle, de la criminalité future ou du « risque » de criminalité représentent une évolution conceptuelle par rapport aux évaluations basées sur des preuves tangibles d'un acte ou d'une implication dans un acte. Ils se concentrent notamment sur un risque imprécis et abstrait qui ***pourrait*** se développer à l'avenir, souvent évalué à partir de preuves circonstancielles et non spécifiques. Ce constat vaut pour tous les systèmes axés sur l'individu ou la personne.

Résultats et impact

Ces systèmes « prédictifs », de profilage et d'évaluation des risques sont utilisés pour influencer toute une série de décisions et de mesures en matière de maintien de l'ordre et d'application de la loi, comme par exemple la surveillance, les contrôles, les interpellations, les interrogatoires, les fouilles, les raids au domicile, et peuvent même conduire à des arrestations.

La police de l'État allemand de Hesse utilise hessenDATA pour faciliter une surveillance intrusive. Bien qu'il ait été conçu pour les crimes « graves », « organisés » ou « relevant de la sécurité de l'État », hessenDATA a été largement utilisé pour des crimes non violents. En 2022, il a été rapporté que la police avait classé environ 12 000 des 14 000 requêtes annuelles de hessenDATA comme « mesures préventives » contre la criminalité.[148]

Les systèmes en question attribuent généralement aux personnes un indice de « risque » faible, moyen ou élevé, ou des variations de ces catégories. Cet indice représente la probabilité présumée que la personne concernée commette une infraction ou se livre à des agissements criminels.

En Allemagne, selon l'Office fédéral de la police criminelle, environ 800 personnes appartenant à la mouvance « islamiste » ont été évaluées par RADAR-iTE depuis 2017.[149] En novembre 2023, 487 personnes impliquées dans des faits criminels « à motivation politique » sous-tendue par une idéologie religieuse ont été classées comme dangereuses (***Gefährder***). En revanche, le nombre de membres d'extrême droite classés comme « ***Gefährder*** » ou « personnes d'intérêt » est encore relativement faible, tout comme le nombre d'évaluations RADAR-rechts.[150]

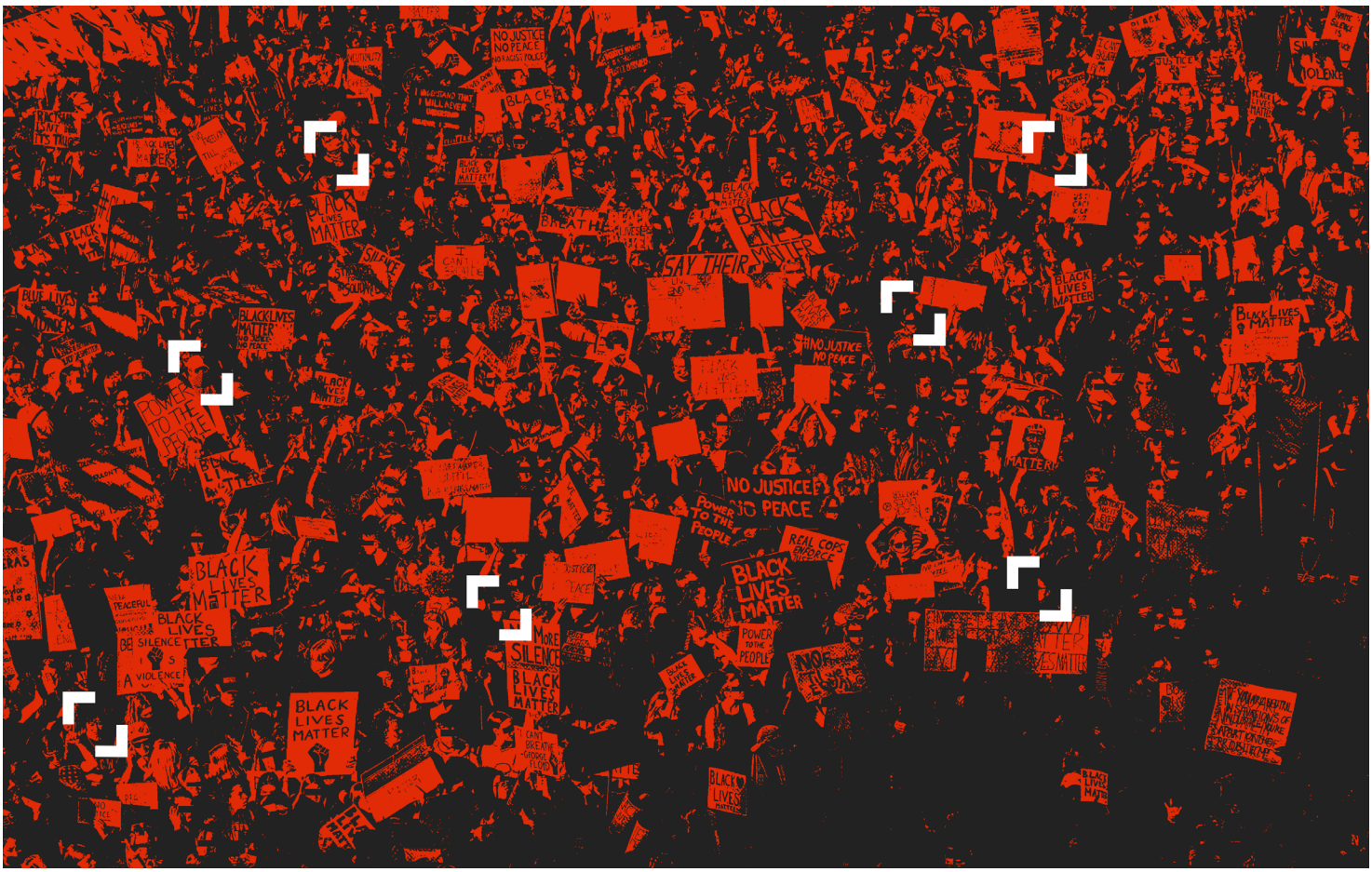
Le système VioGén permet à la police espagnole d'attribuer des scores de risque pour les victimes et non pas pour les délinquants. Un faible score indique que la police communiquera avec la victime par téléphone, tandis qu'un score de risque élevé peut indiquer que la police assurera sa sécurité en surveillant son domicile ou en effectuant des patrouilles.[151] Dans 95 % des cas, les agents de police se conforment aux consignes du système d'évaluation du risque VioGén.[152]

Dans le cadre du profilage des dossiers passagers (Passenger name record, PNR), l'Office fédéral allemand de police criminelle a déclaré que les trajets entre la Turquie et l'Allemagne étaient potentiellement suspects. Selon lui, ces trajets souvent empruntés par des terroristes « islamistes », « sont également très fréquentés par les touristes, peu onéreux et offrent ainsi des possibilités de dissimulation innombrables ».[153]

Le système DRAVY utilisé dans les prisons espagnoles, surestime le niveau de risque pour près de la moitié des personnes qu'il évalue.[154] Ces personnes subissent donc un traitement plus sévère et vivent dans des conditions plus difficiles en prison. Les ressortissants

non espagnols sont ciblés de manière disproportionnée.[155] En Espagne, le système RisCanvi est réputé pour favoriser la discrimination envers les personnes en fonction de leur statut socio-économique ou de leur réseau de relations. Il attribue des scores de risque plus élevés aux personnes qui ont été confrontées à une instabilité professionnelle et financière, qui n'ont pas de famille ni de soutien social et dont les membres de la famille ont des antécédents judiciaires.[156]

Le nombre de personnes ciblées par ce profilage et les conséquences qui en découlent sont considérables.



En septembre 2023, le système VioGén avait évalué environ 770 000 dossiers.[157] Des millions de passagers aériens font l'objet d'un profilage par le biais des systèmes de dossiers passagers (Passenger name record, PNR). En 2022 en Allemagne, 156 compagnies aériennes ont transmis à la police environ 424 millions de données PNR concernant 121 millions de passagers environ. Au 31 octobre 2023, environ 385 millions de dossiers PNR concernant 107 millions de passagers avaient été générés.

De plus, outre la violation de la vie privée de dizaines de millions de personnes, l'utilisation des systèmes PNR a entraîné un grand nombre d'interventions policières. En 2023, les autorités policières allemandes ont effectué plus de 10 000 contrôles en s'appuyant sur le profilage PNR. Presque un cinquième de ces contrôles se sont révélés être de

faux positifs (correspondance incorrecte).[158] Parmi les 8 284 cas positifs (correspondances correctes), les mesures suivantes ont été mises en œuvre :

— 2 178 enquêtes sur le droit de résidence ;

— 2 394 observations policières/contrôles secrets ;

— 1 236 arrestations, 2 303 contrôles ciblés (officiels) ;

— 173 refus d'entrée.[159]

Des millions de données sur les passagers sont analysées afin de mener diverses enquêtes pour des infractions criminelles ou en matière d'immigration, alors que les éléments de preuves sont souvent inexistants ou très minces.

Le rapport sur l'Allemagne met en évidence des exemples concrets qui illustrent les répercussions dramatiques découlant de la classification (erronée) de « ***Gefährder*** ». Les préjugés antimusulmans font que la police et les autorités perçoivent les jeunes musulmans différemment des jeunes hommes de type caucasien ayant un profil de délinquance comparable. Par conséquent, ils sont plus rapidement perçus comme une menace.[160]

Parmi les conséquences du profilage réalisé par le système RADAR-iTE citons :

— la mise sous surveillance et le contrôle ;[161]

— la « détention préventive », dont la durée peut aller de quelques jours à plusieurs mois ;[162]

— la détention avant expulsion[163] et l'expulsion.[164]

Les personnes ayant fait l'objet d'un profilage peuvent également voir leur demande d'asile suspendue.[165]

Autres systèmes de « prédiction » de la criminalité axés sur la personne utilisés en Europe

En plus des exemples décrits ci-dessus, les autorités policières et judiciaires pénales d'autres pays d'Europe utilisent également des outils de « prédiction » de la criminalité et de profilage axés sur la personne. Des travaux de recherche antérieurs ont mis en évidence l'existence de systèmes similaires au sein des services de police et dans les prisons du Royaume-Uni, d'Italie et des Pays-Bas.

Amnesty International UK a récemment révélé que 11 forces de police britanniques utilisaient des outils de « prédiction » de la criminalité et de profilage axés sur la personne ou l'individu.[166] Penchons-nous sur les exemples suivants :

— L'outil « Violence Harm Assessment » de la police métropolitaine de Londres

a été conçu pour profiler des individus à risque de violence à travers Londres. En août 2024, 66 % des individus ayant fait l'objet d'un profilage par le système étaient des personnes noires, tandis que seules 22 % étaient des personnes blanches ;

— Le système de gestion intégrée de la délinquance (Integrated Offender Management, IOM) de la police des West Midlands permet de « prédire » le potentiel futur de délinquance d'un individu. D'après une analyse interne effectuée par le service de police, les personnes noires ont 2,4 fois plus de chances de faire partie de la catégorie « prédite » comme à haut risque de délinquance comparées aux personnes d'Europe du Nord (de type caucasien).

En Angleterre et au Pays de Galles, les services pénitentiaires et de probation utilisent le système d'évaluation des délinquants (Offender Assessment System, OASys) pour « prédire » le risque de récidive de toute personne entrant dans le système de justice pénale. Ce système a fait l'objet de nombreuses critiques pour son profilage racial, la menace qu'il fait peser sur la vie privée et l'absence de responsabilité ou de réparation possibles.[167]

Aux Pays-Bas, la police a utilisé le système ProKid afin de « prédire » le risque de récidive chez les enfants et les jeunes.[168] À Amsterdam, la police a utilisé deux outils de profilage, Top400 et Top600, pour tenter de profiler les « 600 principaux » et les « 400 principaux » mineurs les plus susceptibles de commettre diverses infractions.[169]

Diana Sardjoe, une mère de famille dont les fils ont fait l'objet d'un profilage par Top400 et Top600, a déclaré que ces systèmes ont entrainé une surveillance continue et un harcèlement ciblant ses fils. Elle a notamment appelé à interdire ces systèmes de police « prédictive ».[170]

En Italie, les services de police avaient, dans le passé, employé le système de profilage Delia qui prenait en compte des informations sur l'origine ethnique des personnes à des fins de profilage.[171]

Systèmes de vidéosurveillance algorithmique (basée sur l'IA)

Les forces de police européennes utilisent de plus en plus des systèmes de vidéosurveillance algorithmique ou basée sur l'IA. Ces systèmes s'appuient sur des méthodes d'intelligence artificielle pour analyser des séquences vidéo (p. ex. caméras de vidéosurveillance ou bases de données de la police) dans le but d'identifier des personnes et des objets spécifiques ou de repérer des comportements « suspects ».

Les travaux de recherche qui sous-tendent ce rapport présentent des exemples de systèmes de vidéosurveillance algorithmique utilisés par les forces de police en Belgique et en Espagne. De son côté, ***La Quadrature du Net*** a également effectué des recherches approfondies sur l'exploitation policière de la vidéosurveillance algorithmique en France.[172] En Allemagne, ***AlgorithmWatch*** a identifié deux projets pilotes de systèmes de

vidéosurveillance algorithmique dans les prisons destinés à la « prévention des suicides ». Il existe également des preuves de l'utilisation de la vidéosurveillance algorithmique par la police italienne.

L'usage de la vidéosurveillance algorithmique par les forces de l'ordre suscite de graves préoccupations quant aux violations des droits fondamentaux, en particulier le droit à la vie privée et à la non-discrimination.

Maintien de l'ordre

En Espagne, plusieurs localités de Madrid utilisent des systèmes de vidéosurveillance basée sur l'IA pour la reconnaissance d'images. Ces systèmes, fournis par Bosch Security par l'intermédiaire de la société américaine Intelligent Security Services, ont deux objectifs : la reconnaissance automatique des plaques d'immatriculation (RAPI) et l'identification de personnes suspectées de crimes.[173] Le système peut également rechercher des personnes sur la base de caractéristiques telles que la couleur des cheveux, les vêtements, les traits du visage et l'âge. Il n'existe aucune preuve concrète que le système réduit les taux de criminalité.[174] À Madrid, en janvier 2025, il y avait au moins 83 caméras de surveillance basées sur l'IA exploitées par la police municipale, et la ville a prévu d'en installer 38 autres.[175]

En Belgique, la police locale et fédérale utilise plusieurs systèmes de vidéosurveillance algorithmique, notamment le logiciel développé par BriefCam, une société israélienne, qui permet d'analyser les images rétrospectivement en produisant des résumés vidéo.[176] À l'instar du système Bosch en Espagne, ce système permet à la police de classer les personnes en fonction de critères tels que la couleur des vêtements, le genre ou les effets personnels.

Ce dernier élément pourrait être considéré comme illégal. Le cadre juridique belge en matière de non-discrimination autorise la recherche ciblée sur la base de critères objectifs, mais interdit le triage massif des individus. À la lumière de ces exemples, entre autres, les auteurs du rapport belge préconisent l'abandon de la vidéosurveillance algorithmique dans le cadre du projet à grande échelle « i-Police ».

En 2023, la France est devenue le premier pays européen à légaliser la surveillance biométrique, sous la forme de caméras de vidéosurveillance algorithmiques, dans le cadre d'une loi sur l'organisation des Jeux olympiques de Paris 2024.[177] Le système a été déployé à Saint-Denis. Cette banlieue, au nord de Paris, majoritairement ouvrière avec une présence importante de minorités ethniques, a accueilli la plupart des épreuves olympiques.[178] La législation initiale prévoyait la mise en place de la vidéosurveillance algorithmique jusqu'à fin 2024. Cependant, peu après la clôture des JO, les autorités ont entrepris des démarches pour prolonger son utilisation.[179]

Toujours en France, ***La Quadrature du Net*** a engagé une action en justice de trois

ans contre la commune de Moirans en Isère afin d'interdire la mise en œuvre du logiciel de vidéosurveillance algorithmique Briefcam. Le 30 janvier 2025, le tribunal a rendu sa décision et jugé l'utilisation de ce système illégale. En effet, le logiciel était à l'origine de nombreuses violations en vertu du RGPD et du code français de la sécurité intérieure.[180]

Cette décision rend caduque tout cadre juridique qui autorisait l'utilisation de systèmes de vidéosurveillance automatisée, y compris ceux mis en place à titre expérimental lors des Jeux olympiques de Paris en 2024. Cette décision pourrait faire jurisprudence pour les litiges en cours relativement à l'utilisation des systèmes algorithmiques par la police en France.[181]

Prisons

En Allemagne, ***AlgorithmWatch*** a identifié deux projets pilotes de systèmes de vidéosurveillance algorithmique destinés à la « prévention des suicides » dans les prisons. Ces systèmes de surveillance dignes d'une dystopie viseraient à améliorer la vidéosurveillance actuelle utilisée dans les cellules de prisons en y ajoutant des algorithmes d'apprentissage automatique en vue de détecter les signes avant-coureurs de tentatives de suicide.

En Rhénanie-du-Nord-Westphalie, le ministère de la justice et la société informatique allemande FusionSystems ont collaboré pour développer un algorithme d'apprentissage automatique basé sur des séquences d'entraînement créées par des acteurs. L'algorithme a ainsi été entraîné à détecter des objets (p. ex. couteaux, ciseaux, cordes, briquets, etc.) et les comportements susceptibles d'indiquer des intentions suicidaires. Parmi ces comportements figurent notamment, faire un nœud coulant avec une ceinture, nouer une corde ou attacher un nœud coulant à une grille de fenêtre, sortir un couteau ou utiliser un couteau de grande taille. L'algorithme a également été entraîné avec des séquences de comportements anodins comme s'accroupir, lire ou regarder la télévision. Ainsi, le système devait apprendre à distinguer les situations anodines des indicateurs de risque de suicide.[182] Le système aurait également intégré le suivi du squelette, qui utilise des capteurs et des techniques d'apprentissage automatique pour suivre le mouvement des articulations et du corps d'une personne.[183]

Ces facteurs sont utilisés pour attribuer un « niveau de danger » à une situation au sein d'une cellule qui est ensuite constamment recalculé. Les agents pénitentiaires sont informés de la situation en cours grâce à un système d'alarme visuel à « feux de signalisation ». Une alarme sonore se déclenche si le « niveau de danger » est élevé afin de permettre une intervention rapide.

En Basse-Saxe, le centre de recherche FZI pour les technologies de l'innovation et la société de sécurité informatique VOMATEC Innovations ont collaboré dans le but de développer un système similaire. L'objectif est de produire « un prototype de logiciel opérationnel », qui pourrait être mis en œuvre dans un premier temps dans une prison à Oldenburg.[184]

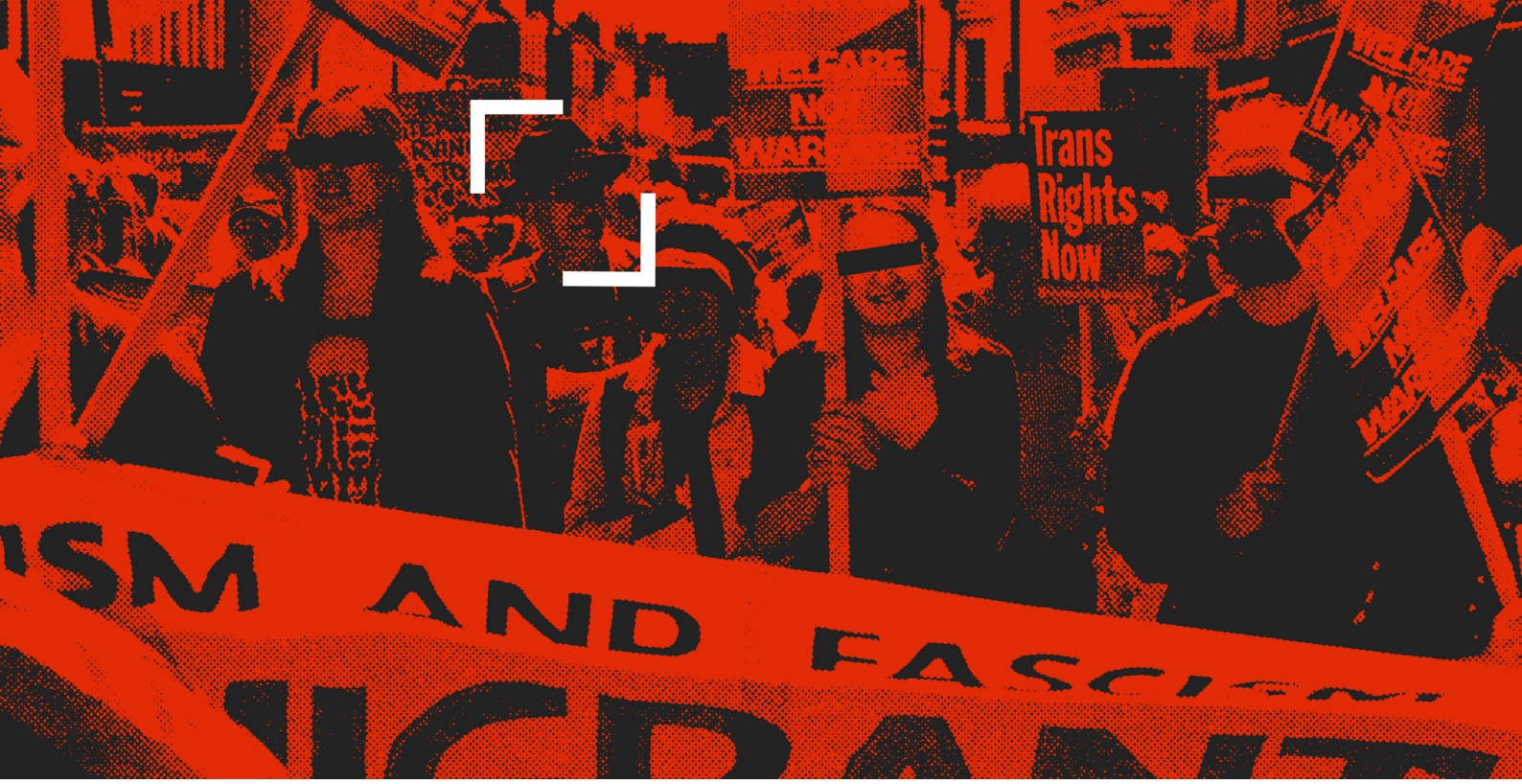
Initialement, le projet visait à appliquer la technologie de surveillance basée sur l'IA dans les espaces communs, tels que les espaces extérieurs ou les espaces de loisirs afin d'identifier, notamment, « le transfert d'objets interdits entre les détenus ».[185] Toutefois, les autorités de protection des données de Basse-Saxe ont émis de sérieuses critiques.[186] Contrairement au système utilisé en Rhénanie-du-Nord-Westphalie, qui a été entraîné avec des images d'acteurs, le système de Basse-Saxe a été entraîné avec des enregistrements réels de tentatives de suicide et de violences dans les prisons.[187]

Les systèmes d'analyse des émotions ou des mouvements corporels basés sur l'IA suscitent également de vives inquiétudes. Non seulement la technologie n'a pas démontré son efficacité sur le plan scientifique,[188] mais elle est également susceptible de renforcer les stéréotypes raciaux ou ethniques. Par exemple, les caméras peuvent être calibrées uniquement pour les tons de peau plus clairs. De même, par rapport aux hommes blancs, les expressions faciales des hommes noirs sont plus susceptibles d'être perçues comme « agressives ».[189] Les biais culturels peuvent influencer notre perception normative des gestes et des expressions faciales. D'autres facteurs peuvent influencer cette technologie, notamment un mauvais éclairage, des visages masqués ou modifiés par des lunettes ou des foulards.

L'utilisation prévue de ces systèmes suscite de graves inquiétudes car les faux négatifs peuvent entraîner des conséquences potentiellement dangereuses. Même s'ils fonctionnent correctement avec des taux de précision adéquats, ils sont très intrusifs[190] et impactent profondément la vie privée des détenus. Un ancien détenu interrogé par ***AlgorithmWatch*** a déclaré que pour prévenir efficacement le suicide, il faudrait abolir le système pénitentiaire :

> *« La prison n'est ni un lieu de thérapie, ni un lieu de réhabilitation : c'est un lieu de punition. Il n'y a donc pas d'aide pour les personnes qui en ont besoin. C'est déprimant et je constate que les gens ne tiennent pas longtemps... Il y a également d'autres moyens de prévenir le suicide : la thérapie et l'empathie, le soutien au sein de la communauté, aider les personnes à trouver un but dans la vie. »*[191]

En 2023, le ministère de la justice espagnol souhaitait mettre en place un projet pilote dans la prison de Mas d'Enric, près de Tarragone, avec des « caméras de reconnaissance faciale et d'analyse vidéo » pour « la détection en temps réel des signes non verbaux et de comportements indicateurs de conduites illicites ». Partiellement financé par l'Union européenne, ce projet devait être étendu à d'autres prisons de la région. Cependant, le gouvernement catalan a annoncé en janvier 2024, qu'à la lumière de la Loi sur l'IA récemment adoptée, il renoncerait à poursuivre le projet.[192]



Bases de données

Les bases de données fournissent souvent les données utilisées dans les systèmes « prédictifs », de profilage et d'évaluation des risques gérés par les autorités policières et judiciaires pénales. Elles peuvent également servir à justifier ou à supposément prouver les mesures prises par la police et les autorités chargées de l'application de la loi. Elles peuvent contenir un grand volume d'informations sensibles couvrant différents groupes de population, comme des renseignements biographiques, des empreintes digitales, des photographies et des antécédents judiciaires, pour ne citer que ces exemples.

En Belgique, il existe plusieurs catégories de bases de données utilisées par la police et les autorités chargées de l'application de la loi :

— la base de données générale nationale est utilisée pour les enquêtes de police ;

— les bases de données « de base » sont constituées des rapport de police sur le terrain et des « renseignements » ;

— les bases de données spéciales sont créées par la police à des fins spécifiques, p. ex. pour cibler les « gangs urbains » ;

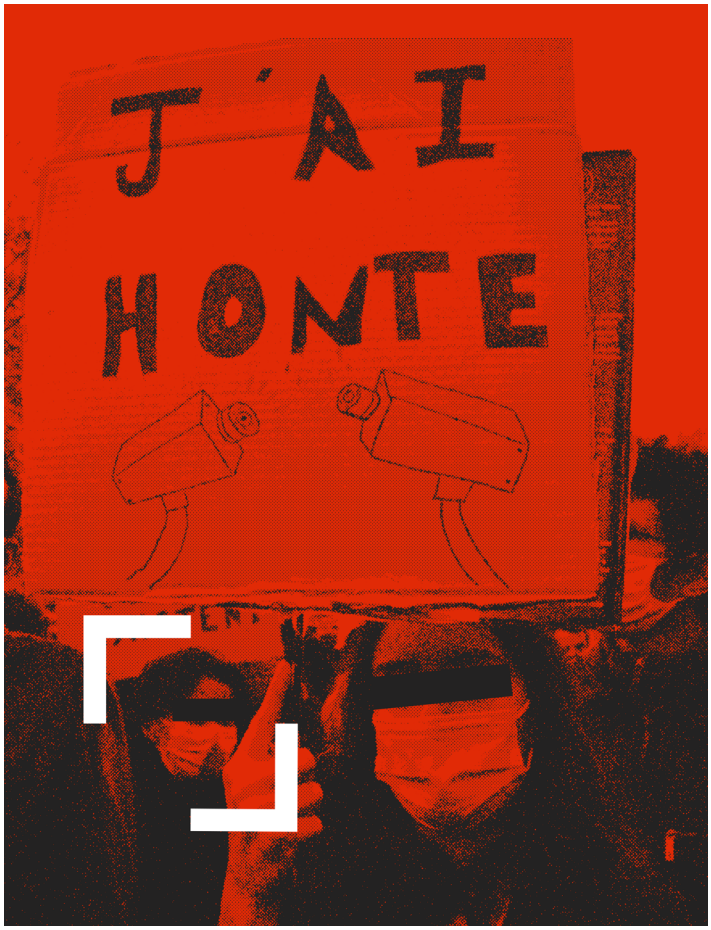
— les bases de données communes partagent des données entre les services de police et de renseignements à des fins supposées de terrorisme ;

— les bases de données techniques contiennent des données collectées automatiquement, telles que celles provenant des caméras RAPI.[193]

En France, la ***Police nationale*** et la ***Gendarmerie*** utilisent la base de données TAJ (« Traitement des antécédents judiciaires ») dans le cadre de leurs activités. Il convient de noter que les autorités françaises ont tenté de connecter cette base de données avec plusieurs autres.[194] TAJ comprend un large éventail d'informations sur les personnes soupçonnées d'avoir commis une infraction grave, ainsi que sur les victimes d'infractions.[195] La collecte illégale de données par la police municipale française est une pratique courante.[196]

La ***Police nationale*** et la ***Gendarmerie*** sont autorisées à utiliser TAJ pour la reconnaissance faciale ***a posteriori*** dans le cadre d'enquêtes judiciaires. Cela signifie que ces services peuvent par exemple prendre des images de vidéosurveillance ou des photos de personnes suspectes et les utiliser pour rechercher des enregistrements correspondants dans la base de données. La fonction de comparaison faciale est également de plus en plus utilisée pour les contrôles d'identité administratifs. En moyenne, le système est utilisé à cette fin plus de 1 600 fois par jour.[197]

ADEXTTRA, la base de données de la police espagnole sur les ressortissants étrangers, contient une liste exhaustive d'informations sur les antécédents. Penchons-nous sur les exemples suivants :



— la nationalité ;

— l'état civil ;

— la profession et les activités professionnelles ;

— la propriété ;

— les revenus ;

— les informations sur le concubinage ;

— le casier judiciaire, les dossiers sur la détention et la détention extrajudiciaire, ainsi que les antécédents criminels ;

— les photographies et autres images ;

— les empreintes digitales ;

— les échantillons de voix.[198]

En Europe, les bases de données utilisées par la police et les autorités chargées de l'application de la loi contiennent d'énormes quantités de données. La base de données générale nationale belge contient des informations sur trois millions de personnes, soit un quart de la population belge.

En France, la base de données TAJ contient près de 20 millions de dossiers de personnes et environ 10 millions de photographies de visages.[199] Créée en 2016 par le ministère de l'Intérieur, la base de données des ***Titres électroniques sécurisés*** (TES) contient des informations sur tous les demandeurs de cartes d'identité et de passeports.[200] Le ministère français de l'Intérieur pourrait, dans un avenir proche, être en mesure d'accéder à l'image faciale de chaque personne présente sur le territoire français.[201] Cette approche s'inscrit parfaitement dans le projet de l'UE visant à collecter des « données d'identité » de chaque ressortissant étranger présent sur le territoire de l'UE, puis à les partager avec les forces de l'ordre et les services d'immigration.[202]

En France, des centaines de services de police municipale utilisent le logiciel « Smart Police », une plateforme et une application numérique conçue pour une utilisation mobile afin de rédiger des rapports, de prendre des photos et de rapporter des évènements qui peuvent ensuite être ajoutés aux bases de données centralisées pertinentes. Smart Police est doté d'un module « prédictif » qui collecte des informations provenant de différentes sources en combinant des données policières sur la criminalité et des données de géolocalisation des agents avec des données socio-économiques sur la population, des prévisions météorologiques, des « rumeurs » provenant de directeurs d'écoles, de bailleurs sociaux ou des réseaux sociaux, dans le but de tenter de « prédire » le risque de criminalité.[203]

Les données stockées dans ces bases de données, ainsi que leur traitement, pourraient avoir un impact très sérieux. En effet, ces bases de données contiennent d'importantes quantités d'informations erronées ou non corroborées présentées comme du « renseignement ».

Le fait d'exploiter des données inexactes semble anodin, mais cela peut entraîner des conséquences très sérieuses. Par exemple, si une base de données contient des informations obsolètes sur une personne, elle pourrait être arrêtée à tort. En Espagne, des migrants ont été détenus par erreur parce que leurs dossiers n'avaient pas été correctement mis à jour dans les bases de données.[204]

Les systèmes « prédictifs » et de profilage peuvent se nourrir de données factuellement exactes, mais aussi d'informations issues des services de renseignement policier. Ces informations peuvent biaiser les résultats de ces systèmes, ce qui peut par la suite influencer les décisions prises par la police et les autorités chargées de l'application de la loi. Les informations non vérifiées sont ainsi traitées comme des faits, qui sont ensuite utilisés contre des personnes.

L'utilisation de ces bases de données soulève d'importantes préoccupations en matière de discrimination illégale. Elles peuvent être discriminatoires ***en elles-mêmes***, en raison de la provenance et des types de données qu'elles contiennent. Leur utilisation peut également conduire à des pratiques discriminatoires.[205] Dans les bases de données gérées par les autorités policières et judiciaires pénales, il y a une surreprésentation significative des personnes, groupes et communautés marginalisés ayant fait l'objet de ciblage, de surveillance et de sanctions de la part des autorités de l'État dans le passé. Il s'agit notamment

des membres des communautés noires et exposées au racisme structurel, des migrants, des personnes issues de la classe ouvrière, de milieux et quartiers socio-économiquement défavorisés, des membres de la communauté LGBTQ+ et des personnes souffrant de problèmes de santé mentale.[206] Plusieurs États fédéraux allemands ont développé des bases de données avec des catégories telles que « junkie », « vagabond(e) », « gitan(e) » et « contagieux(se) », ce dernier qualificatif s'appliquant aux personnes séropositives.[207]

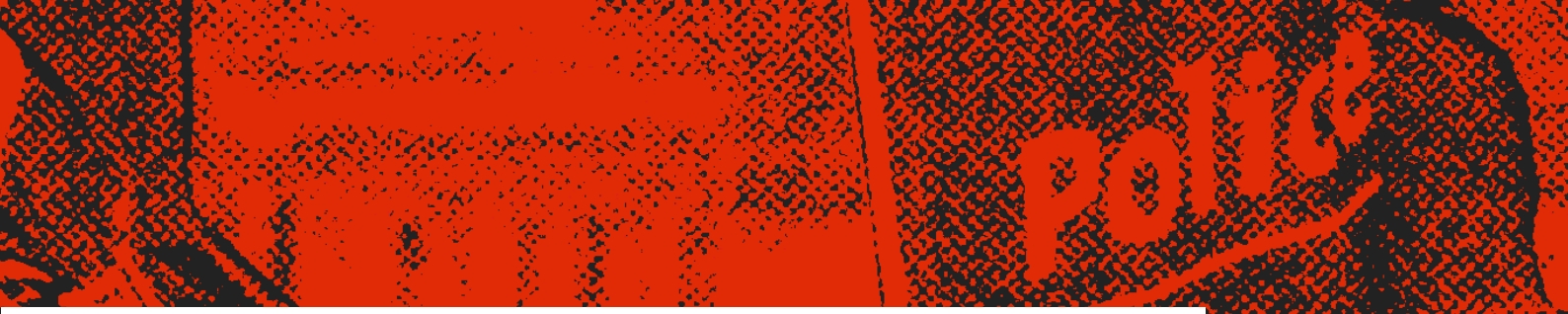
Un nombre croissant d'employeurs et d'autorités utilisent les bases de données de la police belge pour procéder à des contrôles de sécurité. Les personnes d'origine nord-africaine et belgo-marocaine ont davantage tendance à échouer à ces contrôles. Le rapport sur la Belgique évoque également le témoignage d'un jeune musulman qui s'est vu refuser un emploi à cause d'informations erronées contenues dans une base de données de la police.[208]

En Belgique, les services de police au niveau local ont créé des bases de données afin de cibler les « gangs urbains », un terme qui est largement influencé par des stéréotypes racistes et sur les jeunes hommes. Les termes « gangs » et « urbains » ont été utilisés pour classifier ces groupes en raison de leur origine ethnique et les paramètres d'inclusion dans ces bases de données étaient peu clairs. Les personnes incluses dans ces bases de données ont fait l'objet d'un contrôle, d'une surveillance et d'un plus grand nombre d'interpellations et de fouilles.[209]

En Belgique, la police locale gère également des bases de données sur les travailleurs et travailleuses du sexe. Apparemment utilisées pour « réglementer » le secteur, ces bases de données permettent de contrôler et de surveiller les travailleurs et travailleuses du sexe. Dans la mesure où l'enregistrement des travailleurs et travailleuses du sexe est obligatoire, les personnes ayant un statut migratoire irrégulier ou précaire se retrouvent exclues et écartées des réseaux de soutien et de sécurité.[210]

La base de données espagnole ADEXTTRA est utilisée pour identifier les migrants dans le pays et vérifier leur statut. Elle facilite les contrôles d'identité effectués par la police des personnes perçues comme « étrangères ». Il a été amplement démontré que la police espagnole utilise des pratiques de profilage racial.[211]

L'utilisation par la police de ces bases de données et des informations qu'elles contiennent est encadrée par peu de restrictions et de garanties et leur application est également limitée. Les fonctionnaires de police qui consultent illégalement des données ou qui enfreignent les règles et procédures ne sont souvent ni dénoncés, ni sanctionnés.[212] Les délais de conservation des données ne sont souvent pas respectés, ce qui entraîne un stockage permanent et non sécurisé des données personnelles, y compris celles qui pourraient être considérées comme confidentielles.[213] La police ne supprime pas les données qu'elle est légalement tenue de supprimer et il n'y a pas ou peu de mécanismes d'application ou de sanctions en place lorsque cela se produit.[214]



Conclusion

Dans ce rapport, nous avons synthétisé la manière dont les autorités policières et judiciaires pénales européennes mettent en place, utilisent et exploitent des systèmes « prédictifs », avec une attention particulière portée à la Belgique, à la France, à l'Allemagne et à l'Espagne. Parmi les systèmes que nous avons examinés, nous avons étudié les systèmes de « prédiction » de la criminalité et de profilage, ainsi que d'autres systèmes automatisés basés sur des données et systèmes d'analyse de données. Nous nous sommes également penchés sur les bases de données de la police et sur les systèmes de vidéosurveillance algorithmique utilisés par la police et les autorités pénitentiaires.

Il ressort de ce rapport que les forces de police ont de plus en plus tendance à mettre en œuvre des systèmes de prédiction et de profilage, ainsi que d'autres systèmes d'aide à la décision fondés sur des données. Certains de ces systèmes de surveillance proviennent d'entreprises technologiques expertes en la matière. Certaines d'entre elles ont d'ailleurs fait l'objet de controverses en raison de leurs liens avec le gouvernement israélien.

L'utilisation de systèmes de « prédiction » de la criminalité soulève de sérieuses inquiétudes quant à l'augmentation de la criminalisation, des sanctions (y compris des sanctions en dehors du système juridique pénal) et de la discrimination à l'encontre des individus et des communautés marginalisés, en particulier les personnes exposées au racisme et économiquement défavorisées.

Le rapport exprime aussi des doutes importants concernant la précision de ces dispositifs, leur opacité, le manque de responsabilité, ainsi que leur nature potentiellement illégale. Par conséquent, les rédacteurs de ce rapport appuient les demandes formulées par les chercheurs et les organisations partenaires en Belgique, en France, en Allemagne et en

Espagne en faveur d'une interdiction totale de l'utilisation de l'IA et des algorithmes dans l'application de la loi et le système judiciaire pénal, ainsi que d'exigences rigoureuses en matière de transparence et de responsabilité.

Discrimination

Les systèmes « prédictifs » fondés sur une approche géographique ne traitent aucune information concernant des personnes en particulier. En réalité, ce sont surtout les individus exposés au racisme et ceux issus de milieux socio-économiques défavorisés qui sont soumis à des contrôles policiers et à des fouilles, ainsi qu'aux conséquences éventuelles qui en découlent, dans les régions où des faits de délinquance ont été « prédits ».

Ces prédictions entraînent une augmentation de la présence policière et une surveillance accrue des groupes et communautés dans ces quartiers. Cela se traduit par un profilage racial, des interpellations, des contrôles et des fouilles des habitants de ces quartiers et, par conséquent, leur criminalisation. Ainsi, les outils de « prédiction » de la criminalité justifient le ciblage raciste de certains quartiers et de leurs habitants. Ces outils contournent aussi les protections légales censées protéger des pratiques de profilage racial.

Les incidents, ainsi que les contrôles et interventions des forces de l'ordre, sont ensuite enregistrés dans les bases de données qui alimentent les systèmes « prédictifs ». L'utilisation des données pour « prédire » d'autres événements crée un risque d'auto-renforcement qui fait que les mêmes zones et les mêmes profils sont constamment ciblés de manière répétée.

Les systèmes prédictifs axés sur la personne posent le même problème : des données biaisées conduisant à des résultats biaisés et perpétuant ainsi le risque d'auto-renforcement. Par ailleurs, la conception du système espagnol DRAVY fait apparaître une discrimination fondamentale : il se focalise sur le concept occidental de la radicalisation dite « djihadiste » et cible donc presque exclusivement les musulmans et les personnes d'origine musulmane. Il enregistre également un taux important de faux positifs. Le dispositif RADAR-iTE allemand repose lui aussi sur des préjugés islamophobes, ainsi que sur une conception biaisée du danger posé par certaines personnes. Il en découle un préjugé

anti-musulman important en ce qui concerne les résultats obtenus et les personnes concernées.

Criminalisation

Les systèmes de « prédiction » de la criminalité fondés sur une approche géographique désignent des quartiers entiers à haut risque de délinquance avec un taux « prédit » de criminalité élevé. Il en résulte une augmentation de la présence policière, du ciblage, des patrouilles, des interpellations, des contrôles et des fouilles, pour ne citer que ces exemples. La « prédiction » obtenue sert de base en termes de justification et de suspicion. Elle autorise ainsi les contrôles à titre préventif, les contrôles d'identité et les fouilles. Par conséquent, le risque que les personnes et communautés vivant et travaillant dans ces quartiers soient criminalisées augmente. Ce cas de figure peut se produire même en l'absence de preuves tangibles d'infractions.

Les systèmes axés sur la personne réalisent le profilage d'individus en fonction de leurs antécédents. Ils les classent par conséquent directement comme délinquants ou entrainent une stigmatisation indirecte en les considérant comme délinquants potentiels. Ces personnes sont donc coupables jusqu'à ce que leur innocence soit établie. Par ailleurs, il arrive que les systèmes de profilage associent certaines personnes à d'autres qui sont elles-mêmes considérées comme des délinquants. Cette pratique élargit considérablement le champ de la criminalisation.

Les « prédictions » ou profilages ciblant des individus peuvent entraîner des conséquences et sanctions graves, notamment sur le plan de la justice pénale et non pénale. Comme nous l'avons vu dans ce rapport, il s'agit notamment de la surveillance et des contrôles, des visites au domicile ou sur le lieu de travail, des raids, de l'interdiction d'exercer un emploi, des interrogatoires par la police ou les autorités chargées de l'application de la loi, voire des arrestations et détentions « préventives ». Un grand nombre de personnes ont fait l'objet d'enquêtes sur leur statut de résident et ont été soumises à des contrôles aux frontières et à des interrogatoires qui ont entraîné un refus d'entrée, une suspension ou un refus de leur demande d'asile, voire leur expulsion. Tous ces cas de figure peuvent se produire même en l'absence de preuves tangibles d'infractions : juste des soupçons basés sur des données et générés par des algorithmes.

Transparence et responsabilité

Le manque de transparence entourant le développement, l'entrainement et l'utilisation opérationnelle de ces systèmes « prédictifs », de profilage et d'évaluation des risques constitue un obstacle fondamental à la justice et à la responsabilité.

Les personnes ciblées par la police ou les autorités chargées de l'application de la loi du fait de l'utilisation de systèmes de police « prédictifs » ou de « prédiction » de la criminalité ne réalisent généralement pas qu'elles ont été visées. Les autorités qui gèrent ces systèmes ont tendance à ne divulguer aucun détail sur leur fonctionnement ou sur la manière dont ils sont exploités. Elles n'informent pas non plus lorsque des analyses de profilage, de prédiction ou de risque ont été effectuées au sujet d'un quelconque individu, ni si des décisions les concernant ont été prises en fonction de ces analyses. Cela suscite des interrogations concernant l'équité et l'impartialité des systèmes et des procédures qu'ils influencent.

En Europe, aucun cadre juridique n'exige une véritable transparence concernant ces systèmes. La nouvelle Loi sur l'IA de l'UE ne prévoit pas d'exigences de transparence significatives dans ce contexte. Elle inclut toutefois des exceptions majeures pour les systèmes employés dans le but de détecter, prévenir, poursuivre les infractions pénales et enquêter à leur sujet.

Cette situation doit changer. Il est impératif que les autorités policières et judiciaires pénales divulguent des informations détaillées sur tous les systèmes de données, algorithmiques ou automatisés qu'elles utilisent via une base de données ou un site Web accessibles au public. Cela inclut la description du système ou du logiciel, son mode de fonctionnement, les données employées, la manière dont il effectue des analyses ou produit des résultats, ainsi que l'utilisation qui en est faite et les conséquences possibles.

Tout individu ou groupe confronté à des conséquences judiciaires ou pénales découlant de résultats produits par un système d'aide à la décision automatisée ou d'analyses basées sur des données doit être informé de ces conséquences. Les autorités policières ou judiciaires pénales sont tenues d'avertir la personne concernée et lui transmettre les informations pertinentes sur la manière dont elle peut

contester cette décision ou ce résultat. Ces informations doivent être communiquées de manière simple et compréhensible et fournies dans un format clair sans utiliser de jargon technique.

Tout le monde doit pouvoir bénéficier d'un processus clair pour contester des résultats ou conséquences découlant d'un tel système d'aide à la décision automatisée et disposer de voies de recours efficaces.

Absence de base juridique et utilisation illégale

Nombre de ces systèmes controversés sont développés, testés ou exploités sans qu'une base juridique adéquate n'ait été mise en place. Très souvent, ils sont exploités en l'absence de cadre légal et, dans certains cas, ont été jugés illégaux, comme en Allemagne. De plus, la collecte de données qui sous-tend ces systèmes a aussi été jugée illégale, comme en France.

Manque de précision

La plupart du temps, ces systèmes manquent fondamentalement de précision. Ils génèrent des erreurs graves ou des faux positifs, ce qui peut impliquer des personnes innocentes. Dans de nombreux cas, la police, les autorités chargées de l'application de la loi ou le système judiciaire pénal n'ont pas testé de manière significative ou adéquate la fiabilité de ces systèmes avant de les déployer. Même si des tests de ce genre ont été effectués, les autorités en question ont parfois continué d'utiliser des systèmes dont le taux de précision était médiocre.

La précision n'est pas une solution miracle. Un système « précis » ne ferait que renforcer et perpétuer la discrimination inhérente aux données qu'il utilise.

Interdiction

Comme le montre ce rapport, les systèmes « prédictifs » fondés sur une approche géographique et axés sur les personnes, ainsi que les systèmes de profilage et d'évaluation du « risque », mènent au profilage racial et socioéconomique, à la discrimination et à la criminalisation.

L'utilisation de ces systèmes entraîne des conséquences inéquitables et discriminatoires : surveillance, contrôles et fouilles, harcèlement

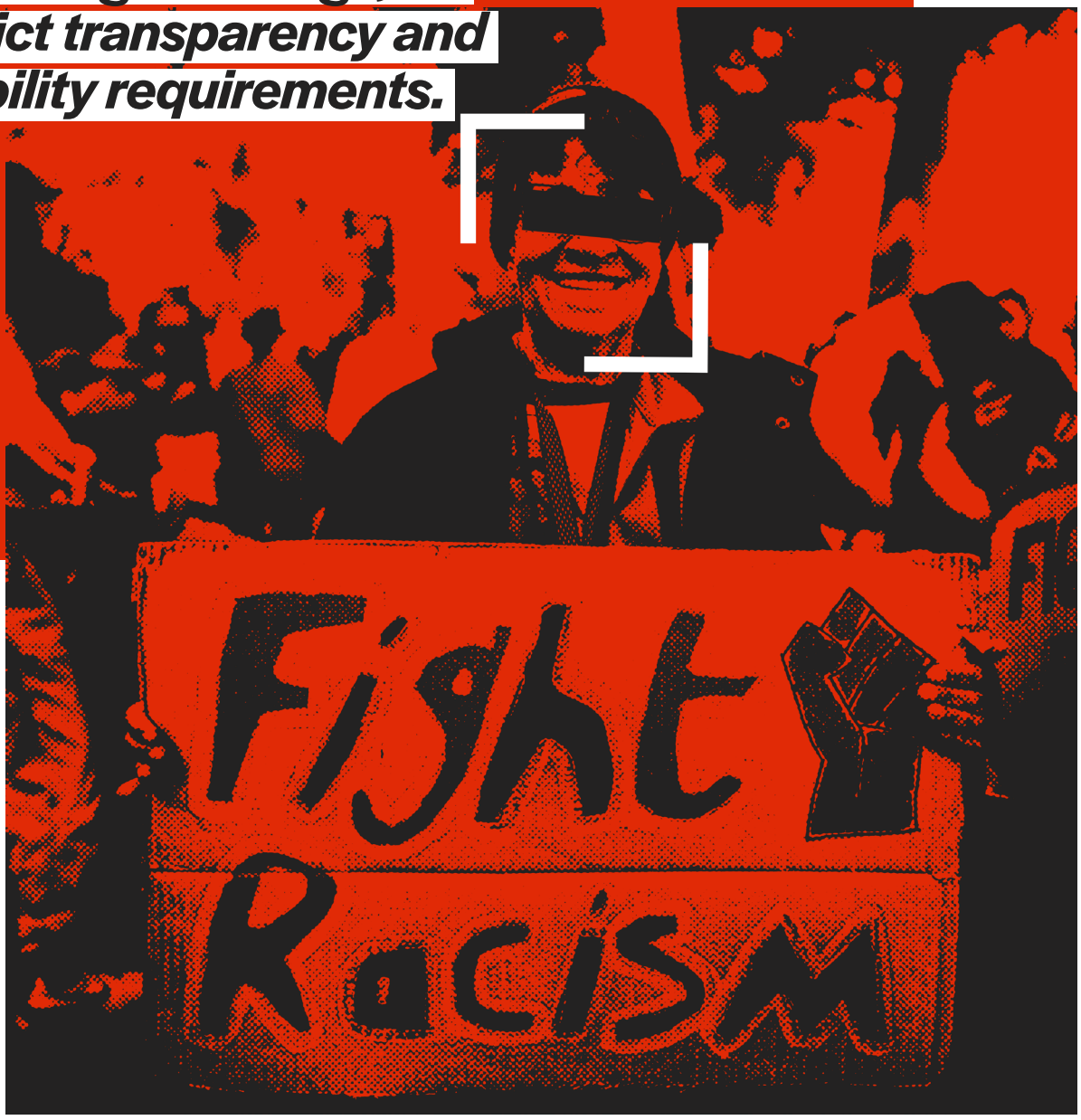
policier, violences, arrestations, détentions et expulsions.

La conclusion de ce rapport et des rapports qui le sous-tendent est claire : il faut mettre fin à l'utilisation de ces systèmes.

Les corps législatifs nationaux des pays où ces systèmes sont actuellement en vigueur devraient légiférer pour les proscrire. De même, les corps législatifs au niveau local, comme les conseils municipaux par exemple, devraient également envisager d'interdire leur utilisation dans leur juridiction.[215]

Depuis des années, plusieurs mouvements luttent pour interdire l'utilisation de ces systèmes en Europe et dans le monde entier. On peut citer notamment la campagne destinée à bannir les systèmes de police prédictive figurant dans la Loi sur l'IA de l'UE,[216] les campagnes ***Technopolice*** en France[217] et en Belgique,[218] la coalition ***Safety Not Surveillance*** au Royaume-Uni[219] et ***Stop LAPD Spying*** aux États-Unis.[220] Il est essentiel de soutenir ces mouvements et ces campagnes, ainsi que d'autres du même type, alors que les gouvernements, les forces policières, les autorités judiciaires pénales et les multinationales cherchent à étendre l'utilisation des systèmes algorithmiques, automatisés et d'intelligence artificielle.

“The authors of this report support the calls of the researchers and partner organisations in Belgium, France, Germany and Spain for a prohibition on all uses of AI and algorithms in law enforcement and criminal legal settings, as well as strict transparency and accountability requirements.



Crédits d'image

Page de couverture: "Politie doet handboeien om" by Shirley de Jong

Page 6: "Brussels police (1)" by Eoghan OLionnain

Page 7: "we won't pay for your greed #2" by Alisdare Hickson

Page 8-11: "Britain's MOD sprayed blood red to highlight the UK's complicity in Israel's war crimes in Gaza #6" by Alisdare Hickson

Page 12: "sscs1014sbab10903" by Santa Cruz Sentinel

Page 13: "Fight Police Racism !" by Alisdare Hickson

Page 14: "Police - Paris, June 1992" by Ian Abbott

Page 15: "Politie overmeestert man" by Shirley de Jong

Page 17: "Palantir pavilion, World Economic Forum, Davos, Switzerland" by Cory Doctorow

Page 18: "manif contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 (1)" by Jeanne Menjoulet

Page 21: "Gendarmerie" by Eddy Meulemans

Page 22: "Spanish Police Colibrí" by José Luis Celada Euba

Page 23: "IMG_4601" by Public Collectors

Page 27: "Greater Manchester Police - BMW R1200RTs" by Autumn

Page 30: "Salt City 21" by Office of Public Affairs

Page 34: "manif contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 (2)" by Jeanne Menjoulet

Page 37: "VIDEO Überwachungsanlage" by Christophe Stoll

Page 38: "Torrevieja police vans ~ repeating patterns dailyshoot" by Les Haines

Page 42: "Protest against doublethink - a peace dove is a paraglider while genocide is self defence" by Alisdare Hickson

Page 44: "Brussels police (2)" by Eoghan OLionnain

Page 46: "#BlackLivesMatter protest in Stockholm, Sweden" by Teemu Paananen

Page 48: "IMG_0297" by Steve Eason

Page 49: "Police surveillance" by York GreenParty

Page 53: "_S9A0303" ****by Steve Eason

Page 54: "manif contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 (3)" by Jeanne Menjoulet

Page 56: "Belgique - 21 juillet 2013 - Police - Politie - Polizei (1)" by Antonio Ponte

Page 57: "Belgique - 21 juillet 2013 - Police - Politie - Polizei (2)" by Antonio Ponte

Page 58-61: "Belgique - 21 juillet 2013 - Police - Politie - Polizei (3)" by Antonio Ponte

Page 62: "manif contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 (4)" Jeanne Menjoulet

Page 63: "Fight Racism !" by Alisdare Hickson

Notes

1 Article 3(1), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_3

2 To give just one example, the definition in the Act is substantially different from the one included in the initial proposal. See: 'Proposal for a Regulation laying down harmonised rules on artificial intelligence', 21 April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

3 Cabinet Office et al, 'Ethics, Transparency and Accountability Framework for Automated Decision-Making', 2021, https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making

4 Cambridge Dictionary, 'Machine learning', https://dictionary.cambridge.org/dictionary/english/machine-learning

5 Amnesty International, 'We Sense Trouble: automated discrimination and mass surveillance in predictive policing in the Netherlands', 2020, https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR3529712020ENGLISH.pdf

6 Links to all the reports are available at: https://statewatch.org/predictivepolicing

7 Lawrence Sherman, 'The Cost-Effectiveness of Evidence-Based Policing', 2010, https://eso.expertgrupp.se/wp-content/uploads/2010/07/2010_3-Sherman.pdf

8 Patrick Perrot, 'L'analyse du risque criminel : l'émergence d'une nouvelle approche', Revue de l'Électricité et de l'Électronique, REE 2014-5 SEE, 2014, https://www.researchgate.net/publication/274071556_L'analyse_du_risque_criminel_l'emergence_d'une_nouvelle_approche.

9 EDRi, 'Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act', 2022, https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/

10 Links to all the reports are available at: https://statewatch.org/predictivepolicing

11 European Union Agency for Fundamental Rights, 'Second European Union Minorities and Discrimination Survey - Main results', 2017, page 26, 29, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-eu-midis-ii-main-results_en.pdf

12 European Union Agency for Fundamental Rights, 'Being Black in the EU — Experiences of people of African descent', 2023, https://fra.europa.eu/en/publication/2023/being-black-eu

13 France 24, 'Police violence: How can France tackle racial profiling without first addressing race?', 9 July 2023, https://www.france24.com/en/americas/20230709-france-s-police-dilemma-how-to-combat-racial-profiling-without-talking-about-race

14 Amnesty International, 'YOU NEVER KNOW WITH PEOPLE LIKE YOU': POLICE POLICIES TO PREVENT ETHNIC PROFILING IN BELGIUM', May 2018, https://www.amnesty-international.be/sites/default/files/bijlagen/ethnic_profiling_executive_summary_en.pdf

15 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019, Report: https://

www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf; Video:

https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain

16 Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022, https://indret.com/wp-content/uploads/2022/07/1715.pdf

17 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020, https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14

18 Samantha Bielen, Peter Grajzl and Wim Marneffe, 'Blame Based on One's Name? Extralegal Disparities in Criminal Conviction and Sentencing', European Journal of Law and Economics, June 2021. DOI:10.1007/s10657-020-09670-6

19 Fair Trials, 'Disparities and Discrimination in the European Union's Criminal Legal Systems', 2021 https://www.fairtrials.org/app/uploads/2021/11/Disparities-and-Discrimination-in-the-European-Unions-Criminal-Legal-Systems.pdf

20 Dieter Burssens, Carrol Tange, and Eric Maes, 'A la recherche de determinants du recours à la detention preventive et de sa duree', Institut National de Criminalistique et de Criminologie, 2015

21 Each One Teach One (EOTO), Citizens For Europe (CFE), 'Afrozensus 2020, Perspektiven, Anti-Schwarze Rassismuserfahrungen und Engagement Schwarzer, afrikanischer und afrodiasporischer Menschen in Deutschland', 2021, https://afrozensus.de/reports/2020/Afrozensus-2020.pdf (translated from German)

22 Germany report

23 Palantir, 'Palantir reports Q4 2024 Revenue Growth', 2025, https://investors.palantir.com/news-details/2025/Palantir-Reports-Q4-2024-Revenue-Growth-of-36-YY-U.S.-Revenue-Growth-of-52-YY-Issues-FY-2025-Revenue-Guidance-of-31-YY-Growth-Eviscerating-Consensus-Estimates/

24 With early funding stemming from In-Q-Tel, the venture capital arm of the CIA, Palantir's customers include: the CIA, NSA, FBI, ICE and army in the US, as well as the NHS in Britain.

25 See here for more information on the company's involvement in the Israeli occupation of Palestine: https://dimse.info/briefcam/

26 See here for information on the use of ClearView software by US police: https://www.bbc.co.uk/news/technology-65057011

27 Edicia, https://www.edicia.fr/fr/

28 Risk Terrain Modelling, https://www.riskterrainmodeling.com/about.html

29 Eurocop, https://www.eurocop.com/. El Salto (2021), 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos'. 4 February 2021. https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas--vigilar-ciudadanos

30 Securitas, https://www.securitas.com/en/

31 See here for more information on SopraSteria's contract with the EU for the 'Shared Biometric Matching System' (sBMS): https://www.soprasteria.com/newsroom/press-releases/details/idemia-and-sopra-steria-chosen-by-eu-lisa-to-build-the-new-shared-biometric-matching-system-(sbms)-for-border-protection-of-the-schengen-area

32 James Bamford, 'How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza', The Nation, 12 April 2024; 'Questions and Answers: Israeli Military's Use of Digital Tools in Gaza', Human Rights Watch, 10 September 2024, https://www.hrw.org/news/2024/09/10/

questions-and-answers-israeli-militarys-use-digital-tools-gaza

33 Forbes, 'Meet The Ex-NSA And Ex-Unit 8200 Spies Cashing In On Security Fears', 10 September 2014, https://www.forbes.com/sites/kashmirhill/2014/09/10/meet-the-ex-nsa-and-ex-unit-8200-spies-cashing-in-on-security-fears/

34 One definition of surveillance tech includes the following wide range of technologies: video surveillance (CCTV systems, IP cameras, video analytics software), big data (data analytics tools for surveillance data, predictive analytics for crime prevention), police body cameras (wearable cameras for law enforcement, recording and storage solutions), biometrics (fingerprint recognition technology, voice recognition systems), domestic drones (aerial surveillance drones for personal use, drones equipped with cameras and sensors), face recognition technology, Radio Frequency Identification tagging, and Stingray tracking devices (for mobile devices and intercepting cellular communications), see: The Business Research Company, 'Surveillance Technology Market Report', 2025. https://www.thebusinessresearchcompany.com/report/surveillance-technology-global-market-report. According to this definition, this report covers only predictive analytics for crime 'prediction', and AI video surveillance.

35 Ibid.

36 Article 5, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_5

37 https://statewatch.org/predictivepolicing

38 Chapter II, Article 5(d), Article 3(1), AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_3

39 EU Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', 4 February 2025, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

40 Fair Trials, 'EU Parliament approves landmark AI law', 16 June 2023, https://www.fairtrials.org/articles/news/eu-parliament-approves-landmark-ai-law/

41 Investigate Europe 'France spearheads member state campaign to dilute European AI regulation', 22 January 2025 https://www.investigate-europe.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation; TIME, 'Big Tech Is Already Lobbying to Water Down Europe's AI Rules', 21 April 2023, https://time.com/6273694/ai-regulation-europe/

42 European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptykon Foundation, and PICUM, 'Artificial Intelligence Act Amendments - Ensure meaningful transparency of AI systems for affected people', November 2021, https://panoptykon.org/sites/default/files/meaningful_transparency_for_people_affected_by_ai_art_52_aia_without_amendment_text.pdf

43 Article 86, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_86

44 Article 50, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_50

45 European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptykon Foundation, and PICUM 'Artificial Intelligence Act Amendments - Ensure rights and redress for people impacted by AI systems', November 2021, https://edri.org/wp-content/uploads/2022/05/Rights-and-Redress-AIA-Amendments-for-online.pdf

46 Article 85, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_85

47 Germany report; Belgium report, France report. France in particular has weak freedom of information laws and performs poorly in the global 'freedom of information' index.

48 Spain report

49 Germany report

50 Braga, Anthony A., Barao, Lisa, 'Targeted Policing for Crime Reduction', Handbook on Crime and Deviance, Handbooks of Sociology and Social Research, Springer, 2019, https://doi.org/10.1007/978-3-030-20779-3_17

51 EU Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', 4 February 2025, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

52 Germany report

53 Knobloch, Tobias, 'Vor die Lage kommen: Predictive Policing in Deutschland', Stiftung Neue Verantwortung, 29 August 2018, https://www.stiftung-nv.de/sites/default/files/predictive.policing.pdf

54 Germany report

55 Germany report

56 Camacho-Collados, M., & Liberatore, F, 'A decision support system for predictive police patrolling'. Decision support systems,75, 25-37, 2015, https://www.sciencedirect.com/science/article/abs/pii/S0167923615000834

57 El Salto, 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos', 4 February 2021, https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas--vigilar-ciudadanos

58 France report

59 Belgium report

60 Orbit GIS, 'Zones de police', https://www.orbitgis.com/fr/zone-de-police

61 The Markup, 'Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them', 2021, https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them

62 Florian Gauthier, 'Prédire les vols de voitures ?', Etalab blog, 2018, https://www.etalab.gouv.fr/predire-les-vols-de-voitures

63 Abgeordnetenhaus Berlin, 'Bericht des Senats gemäß § 21 Absatz 4 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) für das Jahr 2021', 22 July 2022, https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/DruckSachen/d19-0444.pdf (translated from German)

64 France report

65 Germany report

66 Germany report, interview with Egbert, Simon, Postdoctoral Researcher 'The Future of Prediction', University of Bielefeld, 04 October 2023

67 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit', De Standaard. 17 May 2016, https://standaard.be/cnt/dmf20160517_02292901

68 El Salto, 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos', 4 February 2021, https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas--vigilar-ciudadanos

69 Polizei Berlin, 'Kriminalitätsbelastete Orte', https://www.berlin.de/polizei/polizeimeldungen/fakten-hintergruende/artikel.1078268.php

70 Orbit gis. 'Zones de pólice', https://web.archive.org/web/20230930192819/https://www.orbitgis.com/fr/zone-de-police; Orbit gis, 'Zones de police – Stratégie', https://www.orbitgis.com/fr/zone-de-police/zp_strategie

71 Haco. 'Politiezone Westkust experimenteert met datasets in

strijd tegen criminaliteit'. De Standaard. 17 May 2016, https://standaard.be/cnt/dmf20160517_02292901

72 France report

73 Europcop, 'Analysis and prediction of crime', https://www.eurocop.com/sistemas-de-eurocop/analisis-y-prediccion-del-delito/

74 Minister of Interior's answer of 09/07/2020 to written question n°7-591. Belgian Senate, https://senate.be/www/?MIval=/Vragen/SVPrintNLFR&LEG=7&NR=591

75 France report

76 France report

77 Quijano-Sánchez, L, 'Applications of AI and Data Science in Policing: 7 years of collaborations with the Spanish Police'. Lara Quijano-Sánchez, Ph.D by the Politechnic School of the Universidad Autónoma de Madrid. 25 January 2022, https://www.youtube.com/watch?v=z8uBNNPtUmE; Liberatore, F., Camacho-Collados, M., & Quijano-Sánchez, L, 'Towards social fairness in smart policing: Leveraging territorial, racial, and workload fairness in the police districting problem', Socio-Economic Planning Sciences, 87, 101556, 2023, https://www.sciencedirect.com/science/article/pii/S0038012123000563#sec5

78 Ibid.

79 Article 10, Law Enforcement Directive, https://eur-lex.europa.eu/eli/dir/2016/680/oj

80 Recital 38 and Article 11, Law Enforcement Directive, https://eur-lex.europa.eu/eli/dir/2016/680/oj

81 German report, France report, Belgium report.

82 Polizei Berlin, 'Kriminalitätsbelastete Orte', https://www.berlin.de/polizei/polizeimeldungen/fakten-hintergruende/artikel.1078268.php, (translated from German)

83 France report

84 Lina Schmid, 'Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis "kriminilatitätsbelasteter Orte", 2023, in Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird, Nautilus Flugschrift, p.167, translated from German.

85 Süddeutsche Zeitung, 'Unbeteiligte geraten ins Kontrollraster', 12 Sept 2014, https://www.sueddeutsche.de/wirtschaft/ueberwachung-mit-predictive-policing-unbeteiligte-geraten-ins-kontrollraster-1.2115126 (translated from German)

86 Lina Schmid, 'Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis "kriminilatitätsbelasteter Orte", 2023, in Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird, Nautilus Flugschrift, p.167, translated from German

87 Wrangelkiez United, 'Perspektiven: Realitäten von Geflüchteten', Video, https://wrangelkiezunited.noblogs.org/home/, translated from German

88 Ibid

89 George L. Kelling and James Q. Wilson, The Atlantic , 'Broken Windows: The Police and Neighbourhood Safety', 1982, https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/

90 Donna Ladd, 'Inside William Bratton's NYPD: broken windows policing is here to stay', The Guardian, 2015, https://www.theguardian.com/us-news/2015/jun/08/inside-william-bratton-nypd-broken-windows

91 'Northeastern University researchers find little evidence for 'broken windows theory,' say neighborhood disorder doesn't cause crime', Northeastern Global News, 15 May 2019, https://news.northeastern.edu/2019/05/15/northeastern-university-researchers-find-little-evidence-for-broken-windows-theory-say-neighborhood-disorder-doesnt-cause-crime/

92 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf

93 Risk Terrain Modelling, 'Spatial dynamics of crime', https://www.riskterrainmodeling.com/overview.html

94 Ibid.

95 Following its closure in 2020, part of the Observatoire's activities have been transferred to the French Ministry of the Interior's Service Statistique Ministériel de la Sécurité Intérieure (SSMSI, part of the Institut des hautes études du ministère de l'Intérieur or IHEMI, created in September 2020).

96 Camille Gosselin, 'La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique', Paris: IAU Île-de-France, 2019, https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf

97 Belgium report

98 Sûreté Globale website, https://web.archive.org/web/20230610153444/https://www.sureteglobale.org

99 France report

100 Risk Terrain Modelling, 'Spatial dynamics of crime', https://www.riskterrainmodeling.com/overview.html

101 Thibault Sardier, 'Cartographie criminelle : surveiller et prédire', lemonde.fr, 5 January 2018, https://www.lemonde.fr/idees/article/2018/01/05/cartographie-criminelle-surveiller-et-predire_5237723_3232.html

102 Anneleen Rummens & Wim Hardyns, 'Comparison of near-Repeat, Machine Learning and Risk Terrain Modeling for Making Spatiotemporal Predictions of Crime'. Applied Spatial Analysis and Policy, 2021, Vol. 13, no. 4, pp. 1035–1053. DOI: 10.1007/s12061-020-09339-2

103 International terrorism database, https://www.start.umd.edu/gtd/access/. It shows that France only has 20 entries from 2016 to 2019, which leaves one wondering about the relevance of this dataset.

104 France report

105 France report

106 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf

107 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf p.69

108 Ibid.

109 Ibid.

110 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021, https://www.fairtrials.org/articles/publications/automating-injustice/;

111 Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, Justice, Power and Resistance, 5(3), 227-248, https://doi.org/10.1332/UBQA2752

112 AlgorithmWatch, 'The Rise and Fall of a Predictive Policing Pioneer', 7 November 2024, https://algorithmwatch.org/en/predictive-policing-pioneer-keycrime/; Wired, 'Perché la più avanzata startup italiana di polizia predittiva è sull'orlo del baratro', 31 January 2024, https://www.wired.it/article/polizia-predittiva-keycrime-startup-ai-act/

113 Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, Justice, Power and Resistance, 5(3), 227-248, https://doi.org/10.1332/UBQA2752

114 Ibid.

115 AlgorithmWatch, 'Automating Society Report 2020 — Swiss Edition', January 2021, https://automatingsociety.algorithmwatch.org/report2020/switzerland/

116 Belgium report

117 Williams, P, 'Criminalising the Other: challenging the race-gang nexus', Race & Class, 2014, 6(3), 18-35. https://doi.org/10.1177/0306396814556221

118 Belgium report

119 The terms 'terrorist', 'terrorism', 'Islamist', 'extremism', 'extremist' and 'radicalisation' are ill-defined, imprecise and easily misused. As they routinely appear in laws, policies, government statements and academic research, however, they are used in this report for ease of reference. This does not imply that their use or definition by government institutions is endorsed. Per Amnesty UK, 'This Is The Thought Police: The Prevent duty and its chilling effect on human rights', November 2023, https://www.amnesty.org.uk/files/2023-11/Amnesty%20UK%20Prevent%20report%20%281%29.pdf

120 Belgium report

121 'EU: Definition of "potential terrorists" opens door to broad information-sharing', Statewatch, 2 October 2024, https://www.statewatch.org/news/2024/october/eu-definition-of-potential-terrorists-opens-door-to-broad-information-sharing/

122 Bundeskriminalamt, 'RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos)', https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/Radar/radar_node.html

123 Eticas Research, 'The external audit of the VioGen system', 8 March 2022; Bayona, J. Z. (2014). Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo (Doctoral dissertation, Universidad Autónoma de Madrid), https://dialnet.unirioja.es/servlet/tesis?codigo=43479

124 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M, 'Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police'.Knowledge-Based Systems, 2018, 149, 155-168, https://www.sciencedirect.com/science/article/abs/pii/S095070511830128X?via%3Dihub; Nature, 'Police use a computer to expose false testimony', 30 May 2018, https://www.nature.com/articles/d41586-018-05285-9

125 Civio, 'Spanish National Police stop using Veripol, its star AI for detecting false reports', 25 March 2025 https://civio.es/transparencia/2025/03/25/national-police-stop-using-veripol-its-star-ai-for-detecting-false-reports/

126 Germany report; 'PNR for all: UN Security Council mandates worldwide air travel surveillance and profiling, biometric collection, terrorist watchlists', Statewatch, 8 January 2018, https://www.statewatch.org/news/2018/january/un-pnr-for-all-un-security-council-mandates-worldwide-air-travel-surveillance-and-profiling-biometric-collection-terrorist-watchlists/

127 Germany report.

128 Tony Bunyan, 'EU: The surveillance of travel where everyone is a suspect', Statewatch, August 2008, https://www.statewatch.org/media/documents/analyses/no-70-eu-travel-surveillance.pdf

129 European Commission, ''ProtectEU: a European Internal Security Strategy', COM(2025) 148 final, 1 April 2025, https://home-affairs.ec.europa.eu/document/download/48218e1a-9e03-4be1-b19c-d04c323c1117_en?filename=ProtectEU-European-Internal-Security-Strategy_en.pdf

130 Senate, 'Orden de servicio 3/2018', February 2018, https://www.senado.es/web/expedientappendixblobservlet?legis=12&id1=119003&id2=1

131 Andrés- Pueyo, A., Arbach- Lucioni, K., & Redondo, S, 'The RisCanvi: a new tool for assessing risk for violence in prison and recidivism', Handbook of recidivism risk/needs assessment tools, 2018, 255-268, https://onlinelibrary.wiley.com/doi/abs/10.1002/9781c119184256.ch13; AlgorithmWatch (2021), 'In Catalonia, the RisCanvi algorithm helps decide whether inmates are paroled', 25 May 2021, https://algorithmwatch.org/en/riscanvi/

132 Justizportal Nordrhein-Westfalen, § 25a HSOG Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) Landesrecht Hessen, https://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?xid=169564,130; Gesellschaft für Freiheitsrechte, 'NRW Assembly Act: Threat to freedom of assembly and civil-society', https://freiheitsrechte.org/en/themen/demokratie/vb-versammlungsrecht-nrw

133 Germany report

134 Harry Davies, Bethan McKernan, Dan Sabbagh. 'The Gospel': how Israel uses AI to select bombing targets in Gaza', The Guardian, 1 December 2023, www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

135 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019. Report: https://www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf; Video:

https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain; Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022, https://indret.com/wp-content/uploads/2022/07/1715.pdf

136 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020, https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14

137 Jérémiah Vervoort, 'I-Police ou l'art de prédire la discrimination', Travail de fin d'études, Brussels: Université libre de Bruxelles, 2021

138 CERD, 'Concluding observations on the sixteenth to nineteenth periodic reports of Belgium', United Nations Committee on the Elimination of Racial Discrimination. cerd/c/bel/co/16-19, 2014, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%.2F16-19

139 Germany report

140 Welt, 'So funktioniert das Radar für radikale Islamisten', 12 June 2017, https://www.welt.de/politik/deutschland/plus165451390/So-funktioniert_das-Radar-fuer-radikale-Islamisten.html

141 Germany report

142 Germany report

143 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018), 'Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police', Knowledge-Based Systems, 149, 155-168, https://www.sciencedirect.com/science/article/abs/pii/S095070511830128X?via%3Dihub

144 Eticas Research, 'The external audit of the VioGen system', 8 March 2022.

145 Eticas Research, 'The external audit of the VioGen system', 8 March 2022.

146 Tagesschau, 'Immer mehr rechte Gefährder', 26 June 2022, https://www.tagesschau.de/inland/rechte-

gefaehrder-103.html

147 Belgium report

148 Germany report

149 Germany report

150 Germany report

151 Secretary of State for Security, 'Instruction nº 7/2016', 8 July 2016, https://violenciagenero.igualdad.gob.es/wp-content/uploads/Instruccion7_2016.pdf

152 Bayona, J. Z, Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo (Doctoral dissertation, Universidad Autónoma de Madrid), 2014, https://dialnet.unirioja.es/servlet/tesis?codigo=43479

153 Kanzlei Redecker Sellner Dahs, 'Stellungnahme an das Verwaltungsgericht Wiesbaden', 09 September 2021

154 Secretary General of Penitentiary Institutions, Ministry of Interior, 'Construcción y validación de una herramienta de clasificación y de valoración del riesgo de radicalismo violento en el ámbito penitenciario', 2021 https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/instituciones-penitenciarias/Construccion-y-validacion-de-una-herramienta-de-clasificacion-y-de-valoracion-del-riesgo-de-radicalismo-violento-en-el-ambito-penitenciario_126210405.pdf

155 Ibid

156 Karimi-Haghighi, M., & Castillo, C., 'Efficiency and fairness in recurring data-driven risk assessments of violent recidivism', In Proceedings of the 36th Annual ACM Symposium on Applied Computing (pp. 994-1002), March 2021 https://chato.cl/papers/karimi_haghighi_castillo_2021_efficiency_fairness_temporal_recurring.pdf

157 Ministry of Interior, 'Statistical data Viogen', September 2023, https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/violencia-contra-la-mujer/estadisticas/2023/Estadistica-Septiembre-2023.pdf

158 Germany report

159 Germany report

160 Germany report

161 MDR, 'Sachsen-Anhalt will Polizei-Gewahrsam bei Terrorverdacht verlängern', 17 December 2023 https://www.mdr.de/nachrichten/sachsen-anhalt/polizei-gewahrsam-gesetz-aenderung-terrorverdacht-100.html

162 Ibid

163 Tagesspiegel, 'Neue Plätze für 40 Straftäter – im Abschiebeknast', 31 January 2024, https://www.tagesspiegel.de/berlin/losung-fur-berliner-massregelvollzug-neue-platze-fur-40-straftater-im-abschiebeknast-11137660.html

164 Tagesschau, 'Warum die Abschiebepläne kaum einzuhalten sind', 04 October 2022, https://www.tagesschau.de/investigativ/ndr-wdr/koalition-abschiebungen-gefaehrder-101.htm

165 Deutscher Bundestag, 'Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE, Drucksache 19/5202, Personenpotentiale islamistischer „Gefährder"', 9 November 2018, https://dserver.bundestag.de/btd/19/056/1905648.pdf (translated from German)

166 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025 https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20 Amnesty%20International%20UK%20-%202025.pdf?VersionId=JqCcTODw37yAXyINmAY6uAzrKEWucFF7

167 The Conversation, 'A black box' AI system has been influencing criminal justice decisions for over two decades — it's time to open it up', 26 July 2023,

https://theconversation.com/ a-black-box-ai-system-has-been-influencing-criminal-justice-decisions-for-over-two-decades-its -time-to-open-it-up-200594; 'UK: Over 1,300 people profiled daily by Ministry of Justice AI system to 'predict' re-offending risk', Statewatch, 9 April 2025, https://www.statewatch.org/news/2025/april/uk-over-1-300-people-profiled-daily-by-ministry -of-justice-ai-system-to-predict-re-offending-risk/

168 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021, https://www.fairtrials.org/articles/publications/automating-injustice/.

169 Ibid.

170 Fair Trials, 'My sons were profiled by a racist predictive policing system — the AI Act must prohibit these systems', 28 September 2022, https://medium.com/@FairTrials/my-sons-were-profiled-by-a-racist-predictive-policing-system-the-ai-act-must-prohibit-these-b2ea66a9a763

171 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 9 September 2021, https://www.fairtrials.org/articles/publications/automating-injustice/; Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, Justice, Power and Resistance, 5(3), 227-248, https://doi.org/10.1332/UBQA2752

172 La Quadrature du Net, 'Non à la vidéosurveillance algorithmique, refusons l'article 7 de la loi olympique!', 18 January 2023, https://www.laquadrature.net/2023/01/18/non-a-la-videosurveillance-algorithmique-refusons-larticle-7-de-la-loi-olympique/

173 See the 'Law Enforcement and Corrections' webpage on the ISS website: https://issivs.com/served-verticals/law-enforcement-and-corrections/

174 El Pais, 'Marbella, el mayor laboratorio de videovigilancia de España', 22 November 2019, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html

175 La VanGuardia, 'Madrid has 83 cameras on the streets with artificial intelligence Surveillance', 9 January 2025 https://www.lavanguardia.com/mediterranean/20250109/10268393/madrid-83-cameras-street-artificial-intelligence-surveillance-install-mayor-martinez-almeida-spain-city-council-police-technology.html

176 Nicolas Bocquet, 'The Brussels Smart City: how "intelligence" can be synonymous with video surveillance'. Brussels Studies, 2021, journals.openedition.org/brussels/5678

177 La Quadrature du Net, 'France becomes the first European country to legalize biometric surveillance' 29 March 2023, https://www.laquadrature.net/en/2023/03/29/france-becomes-the-first-european-country-to-legalize-biometric-surveillance/

178 Jacobin, 'Emmanuel Macron Is Using the 2024 Olympics to Make France a Surveillance State', 21 March 2023 https://jacobin.com/2023/03/emmanuel-macron-2024-olympics-surveillance-state-ai-biometric-system

179 Jacobin, 'France Wants to Make Olympics-Style Surveillance Permanent', 23 October 2024 https://jacobin.com/2024/10/france-olympics-surveillance-ai-policing

180 ID Tech Editorial Team, 'French Court Rules Briefcam's AI Surveillance System Unlawful', 31 January 2025, https://idtechwire.com/french-court-rules-briefcams-ai-surveillance-system-illegal/

181 Ibid.

182 Ministerium der Justiz des Landes Nordrhein-Westfalen, 'Bericht zum TOP „Todesfälle und Suizide im Strafvollzug. 84. Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 27.10.2021', 25 October 2021. www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-5871.pdf

183 Ibid.

184 Germany report

185 Niedersächsischer Landtag, 'Antrag, Einsatz künstlicher Intelligenz zur Suizidprävention und Verbesserung der Sicherheit in niedersächsischen Justizvollzugsanstalten', Drucksache 18/8729, 09 March 2021, https://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_18_10000/08501-09000/ 18-08729.pdf, translated from German

186 Landesbeauftragte für den Datenschutz Niedersachsen, '27. Tätigkeitsbericht 2021', 2021, https://www.lfd.niedersachsen.de/startseite/infothek/tatigkeitsberichte/2021/barbara-thiel-stellt-tatigkeitsbericht-2021-vor-212174.html, translated from German

187 Germany report

188 Barrett, L. F. et al., 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements', Psychological Science in the Public Interest, 20(1), 1-68, 2019. https://journals.sagepub.com/doi/10.1177/1529100619832930

189 Rhue, Lauren, 'Racial Influence on Automated Perceptions of Emotions', 9 November 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765

190 Article 19, 'Emotional Entanglement: China's emotion recognition market and its implications for human rights', 19 November 2020

191 Germany report

192 AlgorithmWatch, 'Spanish Inmates Not to Be Automatically Monitored in Fear of AI Act', 28 March 2024 https://algorithmwatch.org/en/spanish-inmates-not-monitored-in-fear-of-ai-act/

193 Belgium report

194 Statewatch, 'France: Green light for police surveillance of political opinions, trade union membership and religious beliefs', 13 January 2021, https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-religious-beliefs/

195 France report

196 France report

197 Camille Gosselin, 'La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique', (Paris: IAU Île-de-France, 2019), https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf

198 Ibid

199 Didier Paris and Pierre Morel-À-L'Huissier, 'Rapport sur les fichiers mis à la disposition des forces de sécurité', Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République (Paris: Assemblée Nationale, Commission des Lois), October 2018, http://www.assemblee-nationale.fr/15/rap-info/i1335.asp

200 La Quadrature du Net, 'La reconnaissance faciale des manifestant- es est déjà autorisée', 18 November 2019, https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/

201 France report

202 Statewatch/Platform for International Cooperation on Undocumented Migrants, 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status', 18 November 2019, https://www.statewatch.org/publications/reports-and-books/data-protection-immigration-enforcement-and-fundamental-rights-what-the-eu-s-regulations-on-interoperability-mean-for-people-with-irregular-status/

203 France report

204 Sainz de la Maza Quintanal, E, '"Ultima ratio": el proceso de expulsión de inmigrantes en situación irregular en España', 2015, https://docta.ucm.es/

entities/publication/769b2a6c-8db4-4e2f-8fbe-623cb7c9ce6c

205 Valdivia, A., & Tazzioli, M, 'Datafication Genealogies beyond Algorithmic Fairness: Making Up Racialised Subjects', in Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (pp. 840-850), June 2023, https://doi.org/10.1145/3593013.3594047

206 Belgium report, Germany report, France report

207 Matthias Monroy, 'Suspicion files: German police databases on political activists', Statewatch, 10 April 2018, https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists/

208 Belgium report

209 Belgium report

210 Belgium report

211 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019. Report: https://www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf; Video:

https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain

212 Belgium report, France report

213 Belgium report

214 Belgium report, France report

215 Reuters, 'In a U.S. first, California city set to ban predictive policing', 19 June 2020, https://www.reuters.com/article/us-usa-police-tech-trfn/in-a-us-first-california-city-set-to-ban-predictive-policing-idUSKBN23O31A/

216 EDRi, 'Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act', 1 March 2022, https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/

217 https://technopolice.fr/

218 https://technopolice.be/

219 https://www.openrightsgroup.org/campaign/safety-not-surveillance/

220 https://stoplapdspying.org/