SPECTRE MEDIA

BUSINESS DES FRONTIÈRES

Le Marché aux données

ÉPISODE 1

Novembre 2025

En octobre dernier, une nouvelle base de données européenne est entrée en vigueur. Désormais, tous les citoyens non européens qui franchissent les frontières d'un État membre de l'UE verront leurs données biométriques enregistrées électroniquement dans un système unique. Ce nouveau système de filtrage s'inscrit dans le cadre plus large d'une réforme sécuritaire qui menace les libertés individuelles et le respect de la vie privée.

En expérimentant aux frontières de nouvelles technologies de contrôle, l'Union européenne banalise la surveillance de masse tout en assurant le maintien d'un ordre raciste et capitaliste.

« Légitimer ce type de système ou d'outil à l'encontre des ressortissants étrangers ouvre la voie à l'application de ces mêmes mesures dans d'autres domaines, cette fois contre les citoyens européens. C'est pourquoi chacun devrait se préoccuper de la manière dont son gouvernement traite les étrangers, ou ceux qui tentent d'entrer sur le territoire : car si un État peut agir ainsi envers eux, il pourra aussi le faire envers vous. » **Chris Jones, Statewatch**

Qu'est ce l'Entry/Exit System (EES) ?

Durant les six prochains mois, le système Entrée/Sortie (EES) sera progressivement déployé dans les gares, les aéroports, les ports ainsi qu'aux postes frontaliers extérieurs européens. Lors du franchissement de ces points d'entrée, tous les ressortissants non européens se rendant dans l'UE pour un court séjour (90 jours maximum) devront désormais fournir leurs empreintes digitales ainsi qu'une photo biométrique. Ces informations, ainsi que les données personnelles des voyageurs, seront ensuite enregistrées et stockées dans une base de données européenne centralisée[1].

L'EES s'ajoute aux trois bases de données déjà en place, destinées à assurer la sécurité de l'espace européen[2]. En enregistrant systématiquement les entrées et sorties des ressortissants de pays tiers voyageant dans l'UE, ainsi qu'en identifiant les personnes qui se sont déjà vu refuser l'entrée auparavant, la Commission européenne entend renforcer la surveillance des voyageurs étrangers et repérer plus rapidement, à l'aide d'un système de calcul automatique, les personnes dépassant la durée de séjour autorisée.

Afin de vérifier qu'une personne ne constitue pas une menace pour l'intégrité de l'Union européenne, un logiciel de croisement des données consultera les systèmes d'information européens et internationaux. Pas moins de 700 millions de personnes devraient être concernées par l'analyse et le stockage massif de leurs données.[3]

1. La collecte des informations biométriques sera réalisée au moment de la première entrée dans l'espace européen. Pour les passages suivants, le scan du passeport permettra d'effectuer les vérifications nécessaires (correspondance biométrique de l'identité, potentielle décision de refus d'entrée pour un court séjour) ainsi que l'enregistrement de données personnelles (date et heure d'entrée et de sortie, lieu d'entrée et de sortie, le numéro de passeport du ressortissant, etc.). Ces données seront conservées pour une durée allant de 3 à 5 ans.

2. Eurodac, Système d'information Schengen (SIS), Système d'information sur les visas (VIS). Deux autres systèmes d'informations viendront également dans les prochains mois s'ajouter aux bases de données déjà existantes : le système européen d'information et d'autorisation concernant les voyages (ETIAS) ainsi que le système européen d'information sur les casiers judiciaires (ECRIS-TCN).

3. Schengen News, "EU Confirms Official Entry/Exit System Launch Date", le 19 août 2024.

Qu'est ce que la biométrie et comment cette technologie est-elle devenue un instrument de contrôle des corps ?

La biométrie est un système d'identification fondé sur des caractéristiques physiques propres à chaque individu (empreintes digitales, images faciales, iris, empreintes palmaires, etc.). Cette technologie de gestion des corps s'inscrit dans une longue histoire d'exclusion et de surveillance des populations jugées « indésirables ». Selon plusieurs historiens, ses logiques remontent au système esclavagiste du XVIIe siècle, où les caractéristiques physiques servaient déjà à identifier et tracer les corps noirs durant la traite.[4]

Les technologies biométriques, expérimentées dans les empires coloniaux européens dès la fin du XIXe siècle, ont ensuite été développées pour encadrer, classifier et contrôler les populations colonisées. L'accumulation de données sur les minorités réprimées se trouve au cœur des dispositifs de pouvoir colonial, permettant d'assurer la continuité de la domination.[5] Ces espaces ont vu naître les techniques d'identification de masse, telles que la reconnaissance par empreinte digitale, instaurant un contrôle racialisé des populations. Le perfectionnement de ces techniques d'identification a progressivement contribué à étendre ce dispositif de contrôle à l'ensemble des citoyens des sociétés occidentales.

Aujourd'hui, les données biométriques ne servent plus seulement à identifier le porteur d'un passeport : elles conditionnent l'accès même aux droits que ce document est censé garantir. En combinant ces dispositifs de contrôle et en les universalisant, les États occidentaux ont consolidé un régime frontalier inégalitaire et racialisé, qui réserve aux populations des pays les plus riches un droit effectif à la libre circulation.

Motivées par la volonté de sécuriser l'espace de libre circulation interne, les institutions européennes ont mis en place, dès les années 2000, plusieurs bases de données biométriques contribuant au renforcement des hiérarchies de mobilité. L'extension récente de ces systèmes d'information à grande échelle leur permet d'absorber toujours plus de données et d'élargir le nombre d'acteurs autorisés à y accéder. Ces dispositifs forment aujourd'hui le socle d'une frontière invisible, reposant sur un arsenal technologique de surveillance et de tri des corps.

4. Design -Politics. An inquiry into passeport, camp and borders", Mahmoud Keshavarz, 2016.
5. Arrêt sur image, "La reconnaissance faciale ou l'œil du colonisateur", novembre 2021.

Qu’est ce qu’un « mur virtuel [6]» ?

Un « mur virtuel » désigne un ensemble de dispositifs technologiques destinés à renforcer les barrières physiques et à compléter le travail des gardes-frontières. Le croisement des données, associé à l’usage d’outils informatiques de traitement et d’analyse, permet de trier et de contrôler les personnes avant même leur passage aux frontières. L’utilisation de ces technologies de contrôle s’inscrit dans la stratégie européenne des “smart borders”, amorcée en 2011 par la Commission européenne. Celle-ci prévoit la mise en place d’une architecture technologique ultramoderne, visant à la fois à renforcer la sécurité au sein de l’espace européen et à faciliter la « fluidité » des circulations.

Les bases de données biométriques et leurs logiciels d’exploitation font partie intégrante du déploiement des frontières intelligentes. Présenté comme une condition du maintien de la libre circulation des personnes dans l’espace européen, le recours à ces nouvelles technologies viserait à accélérer la prise de décision et à assurer le suivi des mouvements migratoires, grâce à l’accumulation de données jugées nécessaires à l’évaluation des risques.

Qu’est ce que l’ETIAS et en quoi consiste le système de profilage automatisé ?

Ce nouveau système qui équivaut à l'ESTA américain n'est pas une base de données. Le système européen d’information et d’autorisation concernant les voyages (ETIAS) est un système informatique chargé d'évaluer, à l'aide d'un algorithme, le niveau de risque potentiel que pourrait représenter un voyageur. Cette technologie automatisée, qui s'applique aux ressortissants exemptés de visa, sera chargée de délivrer après un profilage individualisé une pré-autorisation d'entrée dans l'UE. Il vient compléter le système Entrée/Sortie (ESS).

6. TEDx Talks, “Les murs, symboles de frontières”, Damien Simonneau, juillet 2025.

La prise de décision reposera sur l'utilisation d'un algorithme chargé de trier les demandes d'autorisation et d'établir un profil individuel pour chaque voyageur. Le système de fichage des individus s'appuie sur le croisement des informations contenues dans les bases de données européennes et internationales (EES, VIS, SIS, Europol et Interpol), ainsi que sur le recoupement avec une liste de surveillance[7]. Afin d'effectuer son évaluation, le système ETIAS confrontera les données personnelles fournies par les voyageurs à des « indicateurs de risque[8]» définis au préalable par l'unité centrale ETIAS, sous la responsabilité de l'agence Frontex[9]. Selon Amnesty International, les données personnelles librement accessibles sur Internet pourraient également être utilisées par l'algorithme[10].

Même si la réglementation européenne interdit à l'algorithme de prendre en compte l'origine ethnique, la religion ou les opinions politiques pour évaluer le niveau de risque d'une personne, certains voyageurs pourraient malgré tout être catégorisés de manière discriminatoire. Les critères de sélection définis dans l'algorithme d'ETIAS risquent de renforcer les préjugés et d'immobiliser une partie de la population jugée comme présentant un danger potentiel, qu'il soit sécuritaire, sanitaire ou migratoire. En s'appuyant sur une logique de tri automatisé, le système de décision d'ETIAS pourrait accentuer les discriminations déjà présentes dans le régime de circulation mondial.

« Il est évident que votre adresse peut être un indicateur de votre race, car si vous venez d'un quartier majoritairement noir ou asiatique, on peut le déduire. Les critères peuvent donc vous permettre d'attribuer une race. On peut imaginer que les jeunes hommes d'un certain âge vont être signalés plus souvent comme représentant un risque pour la sécurité ». **Chris Jones, Statewatch**

7. Cette liste de surveillance sera mise à jour par l'agence Frontex ainsi que l'agence policière Europol. Ce dispositif de surveillance soulève néanmoins des inquiétudes quant aux abus et au caractère arbitraire des refus d'entrée qui pourraient intervenir suite à la présence du requérant sur cette liste. En réalité, c'est un moyen de contourner la norme européenne en vigueur, car le listing devrait concerner des personnes qui sont « soupçonnées d'être impliquées dans des actes terroristes ou des infractions graves » mais dont les informations ne sont pas assez fondé, justifié pour entrer leurs données dans le Système d'Information Schengen (SIS).
8. Le système d'évaluation des risques repose sur la définition d'indicateurs de risques tels que la tranche d'âge, la nationalité, le pays et la ville de résidence, la destination, l'objectif des voyages, le niveau d'éducation et la profession. Cf. Statewatch, Frontex and interoperable databases: knowledge as power?, février 2023.
9. La réglementation prévoit que les membres du conseil de l'ETIAS définissent quels sont les indicateurs de risques qui contreviennent à la législation. Malgré la présence au sein du conseil d'un comité consultatif des droits fondamentaux, aucun pouvoir contraignant ne lui est attribué.
10. Amnesty International, "Introduction à la défense des droits des réfugié.e.s et des migrant.e.s à l'ère numérique", mars 2024.

Quels sont les risques pour les droits humains ?

Selon la CNIL, les systèmes de décision automatisés présentent des défaillances et sont « susceptibles d'aboutir à des analyses et à prédictions inexactes, voire à des refus de services injustifiés ou à d'autres décisions défavorables aux individus, de perpétuer des stéréotypes et d'enfermer des personnes dans leurs choix[11] ».

Le risque d'exclusion de certaines populations est d'autant plus fort que le Comité pour l'élimination de la discrimination raciale (CERD) a rappelé, dans une série de rapports[12], que les nouvelles technologies ne pouvaient pas s'extraire des structures sociales contemporaines. Dès la phase de conception, les biais raciaux sont ainsi reproduits et incorporés aux systèmes. Le risque de profilage racial, inhérent aux systèmes d'automatisation des décisions fondés sur des bases de données, s'en trouve exacerbé.

Bien que, depuis plusieurs années, les défenseurs des droits humains alertent sur les défaillances des algorithmes, les discours institutionnels continuent de présenter ces technologies comme des outils de gouvernance objectifs et neutres. Si la législation européenne interdit qu'un refus d'entrée sur le territoire soit prononcé sans intervention humaine, le volume élevé de demandes et la pression des décisions automatisées générées par l'ETIAS pourraient influencer fortement la décision finale. De plus, ni l'EES, ni l'ETIAS n'ont fait l'objet d'études d'impact. Il reste donc incertain que le développement de ces technologies, dangereuses pour les droits humains et la protection de la vie privée, ait une réelle incidence sur la sécurité intérieure de l'UE. Le projet ETIAS avait d'ailleurs déjà été évoqué en 2008, avant d'être finalement abandonné par la Commission européenne, qui estimait que « sa contribution potentielle au renforcement de la sécurité des États membres ne justifierait pas la collecte de données à caractère personnel à pareille échelle ni son coût[13] ». Les attentats terroristes de 2015, ainsi que ladite « crise migratoire » ont toutefois réactivé ce chantier, donnant lieu à la création d'une architecture technologique des frontières toujours plus complexe[14].

11. CNIL, "Profilage et décision entièrement automatisée", mai 2018.
12. Comité Comité pour l'élimination de la discrimination raciale, CERD, Discrimination raciale et nouvelles technologies numériques : analyse sous l'angle des droits de l'homme. Rapport de la Rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée* Juillet 2020.
13. Commission européenne, « Frontières intelligentes : options et pistes envisageables », COM(2011) 680 final, 25 octobre 2011.
14. La réforme concernant les systèmes d'information à grande échelle repose sur le concept d'interopérabilité. Elle permet ainsi la mise en réseau des bases de données existantes afin de croiser les informations disponibles. Cette architecture tend à brouiller les frontières entre usages policiers, civils et humanitaires, remettant en cause le principe de proportionnalité selon lequel toute ingérence étatique dans la vie privée doit être justifiée par un objectif légitime et strictement défini.

« Le problème, c'est qu'il s'agit d'une forme de théâtre sécuritaire au sein de l'Union européenne. Ces politiques ne s'attaquent pas réellement aux causes profondes des problèmes, mais traitent plutôt certains symptômes que les gouvernements pensent pouvoir résoudre par l'identification, le suivi et le contrôle des personnes. » **Chris Jones, Statewatch**

La poursuite d'intérêts économiques par des entreprises privées, et leur rôle prépondérant dans le processus de diffusion des technologies de surveillance, soulèvent également des questions majeures quant à leurs responsabilités en matière de protection des données, de respect de la vie privée et de garantie des droits fondamentaux.

Quel est le rôle des entreprises de la tech dans le renforcement des contrôles frontaliers ?

Pour se barricader l'UE n'a cessé d'augmenter le budget alloué à la sécurité des frontières. Selon Euromed Rights, par rapport à la période budgétaire 2014-2020, le montant total des contributions au budget des politiques frontalières de l'UE a augmenté de 94 %[15].

Pour le développement du système Entrée/Sortie (EES), un consortium d'entreprises, comprenant les géants du secteur IBM, Atos et Leonardo, a décroché un contrat de 142 millions d'euros. Le système sBMS (shared Biometric Matching System), élément indispensable au système d'Entrée/Sortie (EES) permettant de croiser les données biométriques entre différentes bases de donnée, a été attribué à Idemia et Sopra Storia pour un contrat de 300 millions d'euros.

Les ambitions politiques européennes, visant à collecter un maximum de données afin d'identifier puis de contrôler les citoyens de pays dits tiers, reposent sur un recours croissant à des entreprises spécialisées qui entretiennent des liens étroits avec le pouvoir. Outre un intense lobbying des entreprises privées, on observe un transfert régulier de technocrates entre les groupes industriels et les institutions européennes. Ainsi, l'entreprise Atos a accueilli dans ses rangs Agnès Diallo, ancienne cadre nommée directrice de l'agence européenne eu-LISA par la suite[16], ou encore Thierry Breton, ancien commissaire européen, qui avait dirigé le groupe avant d'exercer ses fonctions à Bruxelles. Il existe donc un véritable conflit d'intérêts entre les entreprises bénéficiaires des marchés publics liés au développement de ces systèmes et les instances détentrices du pouvoir.

15. Euromedrights, "Europe's Techno Borders", juillet 2023.
16. L'Eu-lisa est une agence gouvernementale européenne, responsable de la gestion des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice. C'est l'institution qui est chargée de l'attribution d'une partie des marchés publics concernant la gestion et le développement des bases de données.

Les politiques sécuritaires de l'Union européenne se construisent avec un petit conglomérat d'entreprises privées devenues indispensables à l'ensemble de la chaîne de développement (stockage des données, maintenance des systèmes, cybersécurité, etc). Les technologies de surveillance, développées notamment grâce aux financements publics européens pour la recherche et le développement, peuvent par la suite être commercialisées et revendues aux États ainsi qu'aux institutions européennes.

L'absence de règles claires encadrant la propagation des nouvelles technologies risque d'accentuer les atteintes aux droits fondamentaux, d'autant plus que les entreprises chargées de leur conception sont déjà impliquées dans le détournement d'outils technologiques à des fins autoritaires.

C'est une tradition de longue date, notamment pour l'entreprise IBM, qui a collaboré avec le régime nazi en mettant en place un système de collecte de données sur les personnes juives facilitant la mise en œuvre de l'Holocaust[17]. Elle est également accusée de complicité dans le génocide en cours à Gaza[18], ou encore suspectée d'avoir vendu au gouvernement Kazakh un logiciel de reconnaissance faciale utilisé pour surveiller et réprimer les opposants au régime[19]. L'entreprise Atos, quant à elle, n'est pas en reste. Sa filiale Amesys a été également mise en cause dans la vente de logiciels de surveillance à des régimes autoritaires, notamment en Libye[20].

Quelles sont les conséquences de tels systèmes à long terme ?

Depuis les attentats du 11 septembre 2001, les discours fondés sur la peur et présentant l'immigration comme une menace pour la sécurité intérieure de l'UE se sont renforcés, justifiant et légitimant davantage le recours à des technologies de surveillance de masse. En imbriquant les enjeux de lutte contre le terrorisme et la criminalité avec les questions migratoires, l'UE et les États membres participent à la construction d'un discours stigmatisant et à la criminalisation des personnes en migration.

17. The Guardian, "IBM 'dealt directly with Holocaust organisers'", mars 2002.
18. Al Jazeera, "UN report lists companies complicit in Israel's 'genocide': Who are they?", juillet 2025.
19. ARTE, "Reconnaissance faciale : des entreprises de la tech au cœur de la surveillance", octobre 2025
20. Franceinfo, "Amesys : qui est ce marchand d'armes numériques français ?", juillet 2017.

Avec l'EES et l'ETIAS, l'Union européenne instaure une suspicion généralisée à l'égard de tous les voyageurs[21]. Il ne s'agit plus seulement de vérifier les identités, mais de surveiller et d'évaluer la légitimité même des individus à circuler dans l'espace européen, au moyen d'un processus de sélection algorithmique. L'introduction de ces nouvelles technologies constitue une pierre supplémentaire à l'édifice d'un espace de libre circulation où les voyageurs jugés « à faible risque » pourront se déplacer sans entrave et en toute sécurité, tandis que les personnes racisées ou marginalisées se verront refuser l'entrée dans l'Union européenne sur la base d'évaluations de risques présumés.

Avec la suppression des barrières frontalières internes, l'externalisation des frontières extérieures, et le renforcement de la surveillance et du contrôle individualisés sont devenus les deux faces d'une même pièce. La construction d'un espace de circulation à deux vitesses s'inscrit dans une gestion raciste des frontières[22]. Ces entraves accentuent les violences frontalières, notamment en provoquant le contournement des dispositifs et en mettant en danger les personnes jugées « indésirables », contraintes d'emprunter des itinéraires secondaires et informels[23].

« Dans un contexte marqué par la montée des gouvernements de droite, de la xénophobie et de l'hostilité envers les immigrés, ces technologies peuvent très facilement être détournées par des gouvernements animés de mauvaises intentions pour identifier et traquer des individus, notamment grâce à la biométrie et à la reconnaissance faciale. Il suffit de se pencher sur l'histoire européenne du siècle dernier pour constater que les registres massifs contenant des informations sur les personnes jugées « indésirables » ont souvent été utilisés par l'extrême droite à des fins profondément abjectes. » **Chris Jones, Statewatch**

21. Statewatch, "Automated suspicion. The EU's new travel surveillance initiatives", juillet 2020
22. Building walls, "Fear and securitization in the European Union", Centre Delàs d'Estudis per la Pau, novembre 2018.
23. "Digital Racial Borders", E. Tendayi Achiume, 2021.

Par la convergence des intérêts économiques et des préoccupations sécuritaires européennes, la surveillance de masse se trouve légitimée pour prolonger le contrôle racialisé des mobilités. Les systèmes informatiques reproduisent et amplifient les discriminations et les inégalités sociales qui traversent nos sociétés, tout en les rendant difficilement contestables, renforçant ainsi le caractère arbitraire des entraves à la circulation.

À la différence du mur, qui conserve une dimension avant tout symbolique, les technologies de contrôle déployées aux frontières se font discrètes et invisibilisent le sort réservé aux personnes en migration. Malgré une dimension éthique profondément préoccupante, ces dispositifs de surveillance façonnent une réalité opaque sans qu'aucun débat sur l'avenir de nos sociétés ne soit initié. En somme, ces systèmes façonnent une nouvelle architecture du pouvoir, où la frontière n'est plus seulement une ligne géographique, mais un dispositif algorithmique capable de filtrer, classer et hiérarchiser les vies humaines.

Contact Presse

- **Autrice -** Maëlle Parfait
- **Fondatrice Specto Média -** Eléonore Plé // contactspecto@gmail.com