# AUTOMATION OF BIOMETRIC CONTROL AND SURVEILLANCE IN PUBLIC SPACE: A RIGHTS-BASED ANALYSIS OF RESISTANCE

**NOVEMBER 2025**

lafede justícia global

EN COLABORACIÓN CON

IA CIUDADANA

AlgoRace
(Des)Racializando la IA

**About this document:**

This document was coordinated by **Laura Riba Singla** and **judith membrives i llorens** (Lafede - Justícia Global), in collaboration with the **Grupo de Trabajo de IA y Espacio Público de la Coalición IA Ciudadana (Working Group on AI and Public Space of the Citizen AI Coalition).**
Authorship of the two analytical articles corresponds to **Paula Cáceres Guerra** (Article 1) and **Youssef M. Ouled (**Article 2), both members of AlgoRace.
The document was designed and laid out by **Isabel Muriedas Díez.**

The purpose of this publication is to support and strengthen the collaborative work undertaken within the state-level coalition.

Translated from Spanish to English by **Najim M. Ouled**.

**With the financial support of:**

European
Artificial Intelligence
& Society Fund

The opinions expressed in this document are the sole responsibility of its authors and of the coalition's working group. The funder does not necessarily share or endorse these views.

**Licence:** This document is released under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International licence. You may use and distribute it provided that proper authorship is acknowledged. To consult a copy of this licence, please visit: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.en

# TABLE OF CONTENTS


Introduction 4

**Article 1:** Biometric Surveillance in Public Space
by Paula Cáceres Guerra 6

**Article 2:** Emotion Recognition and Affective Surveillance in Policing and Migration Contexts
by Youssef M. Ouled 23

Recommendations 36

# INTRODUCTION

This publication is part of the work carried out by the **Grupo de Trabajo de IA y Espacio Público within the IA Ciudadana coalition**, a space that brings together civil society organizations to critically analyze and influence, from a rights-based perspective, the artificial intelligence (AI) technologies that are transforming collective life and to propose political alternatives to surveillance. Our focus is on spaces where power is most visible, such as streets, borders, and police apparatuses, where the automation of social control has its most direct effects on the public, particularly on groups historically subjected to heightened surveillance.

The urgency of this analysis is evident. Europe and Spain are experiencing a rapid expansion of algorithmic surveillance, driven by the deployment of policing and border technologies that combine biometric recognition, behavioral analysis, predictive systems, and mass monitoring. These systems are installed in public spaces such as squares, stations, marginalized neighborhoods, and critical infrastructures, with limited transparency and without meaningful democratic debate. At the same time, the surveillance ecosystem extends to borders and migration management circuits, where technological experimentation is even more aggressive and opaque. In these contexts, AI functions as a filter of mobility, a tool of exclusion, and a mechanism of constant suspicion, reinforcing the criminalization of migrants.

This report pursues a dual objective. First, it seeks to **contextualize European trends within Spain,** identifying how policing surveillance models, digital border control infrastructures, and the institutional narratives that support them are being transferred to the Spanish context. Second, it critically **challenges the security rhetoric that legitimizes these technologies as inevitable solutions,** once again displacing debates about safeguards, proportionality, discrimination, and rights-based alternatives.

The entire analysis is grounded in a human rights and social justice perspective, recognizing that **surveillance does not affect all individuals equally**. It disproportionately impacts racialized youth, migrants, impoverished communities, and territories already subject to intensive policing dynamics. AI, integrated into the management of public space and mobility policies, amplifies these inequalities and consolidates a model of public order based on algorithmic prevention, automated suspicion, and situational control.

Finally, the report connects this analysis to the European regulatory framework, including the European AI Regulation and other relevant EU policies such as the European Pact on Migration and Asylum and the new interoperable database systems, which are shaping a technological governance architecture heavily influenced by a security logic. Although the European AI Regulation introduces certain limits on the use of high-risk systems, its capacity to protect rights will depend on how it interacts with migration and border policies that promote precisely the opposite: more surveillance, more automation, and fewer safeguards. This document explores both the potential and the limitations of the European framework in curbing the expansion of algorithmic control and in creating genuine spaces for accountability and democratic participation.

## Methodological Note

The drafting of the two analytical articles included in this report was carried out by their respective authors, with the support of the **working group** in identifying examples, relevant cases, and applicable regulatory frameworks. This collective support allowed the analyses to be situated within a broader context of institutional practices and regulatory debates in Spain and Europe.

The **final recommendations were developed over two working sessions of the group**, specifically designed to collaboratively construct strategic guidelines aimed at public institutions and key stakeholders. In the first session, the organizations **mapped actors and decision-making spaces,** identifying both the governance levels involved and the agents with potential influence. In the second session, a collective synthesis exercise was conducted to formulate the recommendations, drawing on the findings of the analytical articles and the practical knowledge accumulated by the participating entities.

**The working group wishes to express its gratitude for the generous contribution and commitment of all member organizations,** whose situated knowledge and practical experience were fundamental to the preparation of this report.

# 1. BIOMETRIC SURVEILLANCE IN PUBLIC SPACE

by Paula Cáceres Guerra

## 1. What Is Biometric Surveillance?

In an increasingly automated society, fascinated by the emergence of new technologies and digital innovations, one tool is quietly expanding with little public awareness: **surveillance through biometric systems.** This form of surveillance has evolved into the kind of social panopticism described by Foucault, now transposed into the digital era. It resembles an omnipresent big brother once confined to science fiction, but now capable of becoming a form of social control that may radically transform not only surveillance methods but also their consequences.

To understand what biometric surveillance entails, we must first address the concept of biometric recognition. As defined by Escajedo San Epifanio[1], it consists of "the capture of individuals' bodily attributes" at the metric level. The first official system of this kind, known as Bertillonage, was used by the Paris police in the late nineteenth century to store measurements such as the size of detainees' ears, elbows, or feet in order to determine whether they were reoffending. This system was replaced in the early twentieth century by dactyloscopy, as the collection, classification, and storage of fingerprints proved simpler.

Today, biometric recognition systems cover such a wide and sophisticated range of techniques that many of them appear closer to science fiction than to everyday reality. In addition to fingerprint identification, they include facial recognition (analysis of facial geometry), iris recognition (identification through colour patterns) retinal recognition (analysis of the

1 Escajedo San Epifanio, L. (2025). Vigilancia biométrica masiva mediante IA y derechos fundamentales: retos jurídico-constitucionales. En Balaguer Callejón, F.; Escajedo San-Epifanio, L. Vigilancia biométrica masiva, Inteligencia Artificial y derechos fundamentales (pp. 21-37). Editorial Dykinson.

tissue layer at the back of the eye)[2], **voice recognition** (study of acoustic features such as tone, rhythm and resonance)[3], **vein pattern recognition** (analysis of the veins in the hand using infrared light)[4], and **behavioural biometrics** (analysis of patterns such as walking, handwriting or signing)[5].

From a strictly technical standpoint, biometrics can be understood as a positive and necessary development to the extent that it provides stronger safeguards in areas such as password use or access to bank accounts. The problem is that these systems are being used for purposes that go far beyond the personal sphere. In addition to verifying a singular identity, **biometric recognition is also being used to identify an individual within a group of people, to carry out profiling** (associating a person with a collective), **and to enable large-scale population surveillance** (for example, through cameras installed in public spaces)

This final aspect, surveillance through biometric systems, is highly controversial if we consider that it starts from a complex political premise: **which subjects are deemed worthy of trust and which are deemed worthy of suspicion**. In fact, what has been observed recently is that the political decision about who should be monitored and who should not has ended up transforming the traditional concept of security ("protecting everyone") into a selective form of control ("monitoring only some").

Surveillance systems have always been influenced by biased theories of "criminal identification". This is evident in approaches such as phrenology, physiognomy and deterministic anthropology, as well as in the historical fact that prisons have always been populated predominantly by foreign, racialised and poor individuals. With new biometric surveillance systems that incorporate artificial intelligence and data-processing algorithms, these historical biases of "suspicion" (for example, being Black, poor or a migrant) will be amplified to levels we cannot yet foresee, automating structural discrimination and undermining the rights to personal identity, privacy and equal treatment, all under the mantra of supposed neutrality and efficiency.

Building on the description of biometric recognition mentioned above, biometric surveillance can be defined as the use of technologies that rely on physiological and behavioural data, such as facial recognition, iris recognition, voice recognition or gait analysis, with the purpose of controlling, monitoring and tracking individuals across different environments. With regard to biometric surveillance in public space, this is understood as the large-scale capture of images of individuals in spaces such as airports, squares and streets for various purposes, including border control, the maintenance of public order or the prosecution of criminal offences[6].

## 2. Biometric Surveillance in the European Landscape

### 2.1. Selected Illustrative Cases

Within this context of expanding digital surveillance and securitisation, certain demographic

2 Biometría: lectores de iris y escáneres de retina (s.f.). Cucorent. https://cucorent.com/blog/recursos-humanos/lectores-de-iris/#:~:text=Es%20una%20capa%20de%20tejido%20sensible%20a,extremadamente%20compleja%20y%20%C3%BAnica%20en%20cada%20individuo.

3 Explicación de la biometría sin contacto: métodos y aplicaciones clave (2024). Aratek. https://www.aratek.co/es/news/contactless-biometrics-explained-key-methods-and-applications#:~:text=Tecnolog%C3%ADa:%20La%20tecnolog%C3%ADa%20de%20reconocimiento%20de%20voz,almacenan%20y%20se%20comparan%20para%20su%20autenticaci%C3%B3n.

4 Tipos de sistemas biométricos: la guía completa (s.f.). Recfaces. https://recfaces.com/es/articles/tipos-de-identificacion-biometrica#:~:text=error%20de%20acceso.-,Reconocimiento%20de%20venas,en%20su%20base%20de%20datos.

5 Dispositivos biométrico (s.f.). UNAM, Instituto de Ingeniería. https://www.iingen.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/dispositivosbiometricos.aspx#:~:text=La%20biometr%C3%ADa%20se%20divide%20fundamentalmente,la%20manera%20en%20que%20camina.

6 Galera Victoria, A. (2025). Inteligencia artificial, biometrías y tutela de derechos a la luz del Convenio Marco del Consejo de Europa y la Jurisprudencia del TEDH. En Balaguer Callejón, F.; Escajedo San-Epifanio, L., Vigilancia biométrica masiva, Inteligencia Artificial y derechos fundamentales (p. 276). Dykinson editorial.

groups are being disproportionately affected. This is particularly true for asylum seekers and migrants in an irregular administrative situation, whose biometric data are incorporated into Eurodac, the database shared by all Schengen Area states.

If this system of data collection already represented a clear infringement of the right to privacy and the protection of personal data, **the situation worsened in early 2024 with the adoption of the New Pact on Migration and Asylum.** Among other measures, the reform of Eurodac introduced the following changes: direct access to the database by Frontex, Europol and all police forces across the EU, effectively treating those registered in the system as presumed offenders; the introduction of facial recognition through the capture of facial images, despite the absence of a proper risk assessment and without meeting the prior tests of necessity and proportionality; and the lowering of the minimum age for the application of these technologies from 14 years to 6, meaning that children as young as six will now be included in this database[7].

For decades, Europe has developed and implemented a set of instruments and regulations aimed at closing its borders and exercising racialised surveillance and control over non white populations. Through the reform of Eurodac, and under the claim that it will enable better monitoring of asylum seekers' trajectories, the European Union is further expanding its power over the lives and bodies of people in migratory transit[8].

In addition to Eurodac, other biometric surveillance systems are being implemented or have already been deployed in various European countries. In 2017, the police in Wales (United Kingdom) implemented the AFR Locate project, which consisted of scanning the faces of individuals in public spaces through CCTV cameras during specific events such as the Champions League final, international rugby matches, concerts, or even during the Christmas period on the streets of Cardiff[9]. The aim was to compare the faces captured by the cameras with a watchlist that included individuals sought by the police.

One year after its deployment, the Welsh police themselves released data showing that **nearly ninety two per cent of the identifications made by the system during a 2017 event turned out to be false positives**[10]. In 2019, a Cardiff resident brought legal action against the use of AFR Locate, arguing that it violated his legal rights. The lawsuit was supported by Liberty, the civil rights organisation defending the right to privacy. In 2020, a Court of Appeal ruled that the system did not make clear who could be placed on the watchlist, that no clear criteria existed regarding where it could be deployed, and that no assessment had been carried out to determine whether the software used exhibited racial or gender bias[11]. It is estimated that between 2017 and 2018 the biometric data of at least five hundred thousand individuals were captured without their consent[12].

---

7 El Parlamento Europeo refuerza el control migratorio a través de Eurodac (2022). Algorace.org https://www.algorace.org/2022/12/12/el-parlamento-europeo-refuerza-el-control-migratorio-a-traves-de-eurodac/#:~:text=Adem%C3%A1s%2C%20rebajar%C3%A1%20la%20edad%20de,a%C3%B1os%20o%20de%20por%20vida.

8 Berthélemy, C.; Meyer, L. (2024). Tu cuerpo como pasaporte: la pesadilla biométrica en el corazón del sistema de asilo de la UE. La Marea. https://www.lamarea.com/2024/04/08/tu-cuerpo-como-pasaporte-la-pesadilla-biometrica-en-el-corazon-del-sistema-de-asilo-de-la-ue/

9 Cotino Hueso, L. (s.f.). Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos. Fundación Jiménez Abad. www.fundacionmgimenezabad.es/sites/default/files/Publicar/publicaciones/documentos/oc27_13_lorenzo_cotino_es_o.pdf

10 Corte del Reino Unido califica programa de reconocimiento facial como ilegal (2020). Red de Defensa de los Derechos Digitales. https://r3d.mx/2020/08/13/corte-del-reino-unido-califica-programa-de-reconocimiento-facial-como-ilegal/

11 Cox, K. (2020). El uso del reconocimiento facial por parte de la policía viola los derechos humanos, según un tribunal británico. ARS Technica. https://arstechnica.com/tech-policy/2020/08/police-use-of-facial-recognition-violates-human-rights-uk-court-rules/

12 La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleado por el sector público (s.f.). Consejo para la Transparencia. Dirección de estudios / Dirección Jurídica.

Another noteworthy example is the SARI Real-Time project, promoted by the Italian government, which sought to install cameras in designated geographical areas in order to compare the facial images captured in those locations with a predefined database (referred to as a watchlist) of ten thousand faces. Once the system detected a match between a face on the watchlist and a face captured by the cameras, an alert would be issued to notify law enforcement authorities. However, in 2021 the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali - GPDP) declined to authorise the use of SARI Real-Time, on the grounds that it **lacked a legal basis for the automated processing of biometric data for facial recognition in the context of surveillance, and that it amounted to a form of indiscriminate, mass surveillance.** The GPDP also noted that the system could affect individuals merely attending social or political demonstrations who were not in any way subject to police monitoring[13].

More recently, in 2023, France adopted a provision within the framework of a draft law concerning the 2024 Olympic and Paralympic Games to authorise the experimentation of algorithmic video surveillance until 2025 in the context of sporting, cultural, and recreational events involving more than three hundred participants. The stated objective was to detect suspicious behaviour in real time within large crowds[14]. La Quadrature du Net, an organisation specialising in data protection and digital rights, argues that, despite the government's claims that the project would not use biometrics, the technology will identify and classify physical attributes, silhouettes, gestures, and gait patterns, which are "undeniably biometric data"[15], and will do so on the basis of "suspicious behaviours" defined arbitrarily in advance by the police.

Lastly, in May 2025, Hungary approved a bill prohibiting Pride parades and, for the purpose of identifying attendees, authorising the use of facial recognition software[16].

These examples demonstrate not only the failures of such systems but also their **clear implications for individual rights.** Nevertheless, the European Union continues to push for the deployment and expansion of these technologies. Indeed, the EU's biometric Entry/Exit System (EES) is scheduled to become operational in 2025 and will be gradually implemented from October of this year onwards. The EES will apply to nationals of third countries entering the Schengen Area, who will be required to provide fingerprints and facial images at the moment of crossing the border.

This system will replace the current manual passport stamping procedure with an automated digital record, enabling real-time access to travellers' data in order to prevent irregular entry and identify individuals who overstay the permitted period[17].

Among the main arguments invoked to justify the implementation of the EES is the **well-worn triad of counterterrorism, national security, and the migration threat**, a premise that ultimately serves to legitimise systems that consistently target the same demographic groups. Migrants, displaced persons, and asylum seekers, who are already experiencing significant social vulnerability, will now also face the automated stigmatisation and criminalisation embedded in the operation of the EES.

13 Reconocimiento facial: Sari Real Time no cumple con las normas de privacidad (2021). Garante per la Protezione dei Dati Personali - GPDP. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842

14 Gibon, C. (2023). Francia quiere vigilar a las multitudes con la ayuda de inteligencia artificial y algoritmos durante los JJOO de París. Equal Times. https://www.equaltimes.org/francia-quiere-vigilar-a-las?lang=es

15 Francia, primer país de Europa en legalizar la vigilancia biométrica (2023). La Quadrature du Net. https://www.laquadrature.net/2023/03/23/la-france-premier-pays-deurope-a-legaliser-la-surveillance-biometrique/

16 Hungría: La prohibición del Desfile del Orgullo, un ataque frontal contra las personas LGTBI que no debe convertirse en ley. Amnistia Internacionak, https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/hungria-la-prohibicion-del-desfile-del-orgullo-un-ataque-frontal-contra-las-personas-lgbti-que-no-debe-convertirse-en-ley/

17 The role of the biometrics in the European Entry-Exit System (s.f.). Laxton. https://www.laxton.com/es/blog/the-role-of-biometrics-in-the-european-entry-exit-system/

## 2.2. State of Legislation

The rapid development of artificial intelligence technologies has been accompanied by several legislative initiatives aimed at regulating their design and use. The most recent was the adoption of the Artificial Intelligence Regulation (AI Act) by the European Parliament, which entered into force in August 2024. This regulation classifies AI systems according to the level of risk they pose to fundamental rights: unacceptable (and therefore fully prohibited), high, limited, and minimal[18].

The AI Act was adopted with the aim of regulating the uses of artificial intelligence and ensuring that systems placed on the EU market are safe and respect fundamental rights and European values[19]. With regard to biometric identification, **the regulation prohibits its real time use in public spaces for law enforcement purposes, as these systems are considered to pose an unacceptable risk to individuals' rights**. It also prohibits the creation or expansion of facial recognition databases using images taken from the internet or from closed circuit television.

As for remote biometric identification (that is, using devices operated at a distance from a control room, for example), which is classified as a high risk system, the AI Act authorises its use when required for medical or security purposes[20].

This last point is particularly contentious because the AI Act establishes a general exemption from the entire regulation for reasons of "national security." This means that the law does not have to be applied when systems are developed or used for security purposes, regardless of whether this is carried out by a public entity or a private company, which are thereby exempt from review and scrutiny. European Digital Rights (EDRi) asserts that, in practical terms, **governments will be able to invoke national security to deploy mass biometric surveillance systems without implementing any of the safeguards provided by the law,** without conducting impact assessments, and without ensuring non discrimination towards specific groups of people[21].

This exemption effectively creates a kind of parallel regulatory framework for border and migration control contexts, as well as for other scenarios that may fall under the concept of "national security," demonstrating, once again, that categories of people, first or second class, are established based on their origin. Given that national security concerns are often linked to borders with countries in the Global South or to individuals originating from or associated with these geographic regions, an undeniable racial factor underlies the concept of "national security".

Another regulatory framework in this domain is the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, adopted in May 2024, which aims to establish common principles and rules "to ensure the protection of human rights, democracy and the rule of law in relation to activities throughout the lifecycle of artificial intelligence systems."[22] This convention is structured in eight chapters, highlighting Respect for human dignity and individual autonomy, Equality and non-discrimination, Respect for privacy and protection of personal data, Transparency and oversight, Accountability and responsibility,

18 Guerra, P. (2023). Por qué es importante la Ley de Inteligencia Artificial. Eldiario.es https://www.eldiario.es/opinion/tribuna-abierta/importante-ley-inteligencia-artificial_129_10602479.html

19 Galera Victoria, A. (2025). Inteligencia artificial, biometrías y tutela de derechos a la luz del convenio marco del Consejo de Europa y la jurisprudencia del TEDH. En Balaguer Callejón, F.; Escajedo San-Epifanio, L. Vigilancia biométrica masiva, Inteligencia Artificial y derechos fundamentales (pp. 269-300). Editorial Dykinson

20 ¿Qué dice la Ley europea de Inteligencia Artificial sobre los sistemas que usan datos biométricos? Algunos están completamente prohibidos y otros permitidos bajo ciertas obligaciones (2024). Maldita.es https://maldita.es/malditatecnologia/20240814/ley-ia-ue-sistemas-biometricos/

21 La Ley de IA de la UE no establece un estándar de oro para los derechos humanos (2024). Edri.org https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/

22 Decisión (EU) 2024/2218 del Consejo, de 28 de agosto de 2024, relativa a la firma, en nombre de la Unión Europea, del Convenio Marco el Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho. Boletín Oficial del Estado, 4 de septiembre de 2024, pp 1 a 3. https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81308

Reliability, and Safe innovation. However, like the AI Act, the Convention excludes from its scope "activities throughout the lifecycle of AI systems related to the protection of national security interests and national defence matters," regardless of the type of entity carrying out these activities [23].

Both the AI Act and the Council of Europe Convention invoke the concept of national security to justify the often experimental, indiscriminate and uncontrolled use of biometric surveillance technologies over populations in particular social vulnerability, such as people in migratory transit or asylum seekers. In doing so, they reinforce the advance towards a biometric policing state, where the line between security and social control becomes dangerously blurred.

### 2.3. Collective Struggles and Resistance

In response to this situation, several organisations and collective initiatives have emerged to curb the expansion of indiscriminate facial recognition technologies. Three of the most significant are:

- *Reclaim Your Face* (RYF), an initiative that brings together more than seventy organisations and whose mission is to advocate for the prohibition of mass biometric surveillance in public spaces within the EU. On its website, RYF states that the combination of biometric data and mass surveillance results in all individuals being treated as suspects and constitutes a violation of the rights to freedom of assembly, expression, and non discrimination. They also warn that this type of surveillance causes people to modify their behaviour, becoming demobilised and self censoring, a phenomenon known as the "chilling effect", which generates an imbalance of power between citizens and those who monitor and categorise them [24]. RYF has collected nearly eighty thousand signatures in support of the European Citizens' Initiative (ECI) for the legal prohibition of biometric technologies that may lead to mass surveillance.

- *Protect not surveil (PnS)*, s a coalition composed of activists, organisations, and researchers working to ensure that the AI Act protects migrants and racialised communities from harms arising from artificial intelligence systems. They challenge the use of digital technologies in European policies and defend the right of individuals to move and seek safety and opportunities without being subjected to surveillance or discrimination. Their work approaches these issues from a perspective that integrates digital rights and the rights of migrants [25].

- All Out is a European campaign advocating for the prohibition of automated recognition of gender and sexual orientation. On its website, the campaign points out that many AI systems classify individuals based on a binary understanding of gender and operate under the mistaken assumption that gender and sexual orientation can be inferred from appearance. They argue that this can lead to errors that foster discrimination against LGBTIQ+ communities or have severe consequences if such technologies are used in countries with anti LGBTIQ+ laws. For this reason, the campaign emphasises the need to ban facial recognition algorithms for the purpose of identifying gender or sexual orientation [26].

Another notable aspect of resistance and collective struggles is strategic litigation, which allows the judicial system to be used to generate broad and long term social change, establish legal precedents, and influence future public policies.

---

23 Ibid.
24 Los poderosos observan a los débiles (s.f.). Reclaimyourface.eu https://reclaimyourface.eu/the-problem/
25 La UE debe poner fin al uso de tecnología de vigilancia contra las personas migrantes y las comunidades racializadas (s.f.). Protectnotsurveil.eu https://protectnotsurveil.eu/index_es.html
26 Ban automated recognition of gender and sexual orientation (s.f.). All out.org https://campaigns.allout.org/ban-AGSR?_ga=2.132562957.2022005740.1643728362-441876419.1643728362

An interesting case, previously mentioned in the example from the United Kingdom, was the legal action brought by Edward Bridges against the police in Wales regarding the use of the real time facial recognition system called AFR Locate. This system began operating in 2017 in public spaces and during sporting, cultural, or high footfall events during the Christmas period on the streets of Cardiff. The aim was to compare faces captured by the cameras with a watchlist that included individuals sought by the police. In 2019, Bridges initiated a judicial review of the technology, arguing that the use of AFR Locate violated Article 8 of the European Convention on Human Rights, as well as the United Kingdom's Data Protection Act 2018. He also contended that the police had failed to meet their obligations regarding equality under the Public Sector Equality Duty (Equality Act 2010)[27].

Bridges was supported by Liberty, the civil rights organisation defending the right to privacy. In a first instance ruling, the Administrative Court of the High Court of Justice held in 2019 that, while facial recognition technology did compromise the protection of individuals' data and the right to privacy, its use by the police fell within their powers to prevent and detect crime[28].

The following year, in 2020, the Court of Appeal of England and Wales upheld Bridges' appeal and overturned the first instance ruling, arguing that the use of AFR Locate had "fundamental deficiencies" due to its excessive discretion, the absence of impact and risk assessments, and the lack of measures to address potential indirect discrimination in cases of error[29].

Another case worth highlighting took place in New York City, after the Supreme Court ruled in favour of Amnesty International and the Surveillance Technology Oversight Project (STOP). The organisations had sued the City Police Department, which was then ordered to release thousands of documents demonstrating that the police had acquired and used facial recognition technology against protesters from the Black Lives Matter (BLM) movement[30].

## 3. Current Situation in Spain

### 3.1. Some Documented Cases

Within this context of increasing digitalisation of societies, Spain has not escaped the rise of facial recognition in matters of surveillance and security, both in private and public sectors, as evidenced by several examples.

In 2019, a court in San Sebastián authorised a supermarket in Irun, Gipuzkoa, to install a facial recognition system in order to enforce a court ruling that prohibited two women convicted of theft from approaching the establishment[31].

In another case, in 2021, the Spanish Data Protection Agency (AEPD) opened administrative

27 La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleado por el sector público (s.f.). Consejo para la Transparencia. Dirección de estudios / Dirección Jurídica. https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf

28 Ibid

29 Control judicial de los algoritmos (2023). Asociación profesional de la magistratura (APM). Magistratura.es https://magistratura.es/control-judicial-de-los-algoritmos- por-alfonso-peralta-gutierrez/

30 Estados Unidos: Tras una demanda judicial, la policía de NY recibe la orden de entregar documentación relativa a la vigilancia de las protestas de BLM. Amnistía Internacional. https://www.amnesty.org/es/latest/news/2022/08/usa-nypd-black-lives-matter-protests-surveilliance/

31 Permiten a una tienda sistema de reconocimiento facial para evitar a dos ladronas (2019). La Vanguardia. https://www.lavanguardia.com/vida/20190614/462862950020/permiten-a-una-tienda-sistema-de-reconocimiento-facial-para-evitar-2-ladronas.html

proceedings against Mercadona for implementing a pilot facial recognition system in forty of its stores, aimed at detecting individuals with final convictions or active restraining orders [32]. The AEPD argued that the processing of data based on facial recognition for identification purposes, as carried out by Mercadona, is prohibited under Article 9 of the Spanish General Data Protection Regulation (GDPR), and subsequently imposed a fine exceeding two and a half million euros [33].

The following year, AENA announced that it was implementing biometric technology to allow boarding of aircraft without any identification method other than the passenger's face, in order to provide travellers with a "more agile and secure" experience[34]. To carry out this procedure, AENA records the traveller's image in a selfie format, alongside the passport or national identity document, as well as personal data and the chip image of the identification document, in order to verify identity and document validity[35]. At the time of closing this text, the AEPD has fined AENA for this implementation[36].

In another example, in 2023, the National Police began using a facial recognition system called ABIS, developed by Thales, a French military technology company. ABIS operates by searching for matches between images submitted by police officers, which are obtained from mobile devices, security cameras, or photographs, and the databases of the Guardia Civil and the National Police, which contain data on more than four million individuals who have been detained [37].

In 2024, the Ministry of Health implemented an artificial intelligence system with facial recognition of patients in Ceuta and Melilla, aimed at avoiding duplications, impersonations, and other problems arising from patient identification[38]. According to the organisation **Civio**, the number of potentially affected individuals could reach 170,000, including Social Security affiliates, mutual society members, "and non affiliated foreigners, mainly Moroccans"[39].

These cases are complemented by the so called *smart border* at Spain's southern frontier. In February of this year, the Minister of the Interior, Fernando Grande Marlaska, inaugurated the facilities at the Beni Enzar border crossing, which separates Melilla from Morocco, stating that the new system would provide a more efficient and secure screening process[40]. A month later, it was reported that the system was fully operational in Ceuta[41].

---

32 La protección de datos personales en contextos de avanzado desarrollo tecnológico (s.f.). Consejo para la Transparencia. Dirección de estudios / Dirección Jurídica. https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf

33 Ibid

34 Biurrun, A. (2022). Así es la tecnología biométrica de AENA con la que podrás coger un avión sin mostrar ninguna documentación. La Razón. https://www.larazon.es/tecnologia/20220810/fiyg44hisbfghoy6sra53l3khi.html

35 Ibid

36 Javier F. Magariño. Protección de Datos multa a Aena con 10 millones por la identificación biométrica de los viajeros y abre un frente en los tribunales. El País. https://elpais.com/economia/2025-11-25/aena-se-revuelve-ante-los-10-millones-de-multa-de-la-agencia-de-proteccion-de-datos-por-la-identificacion-biometrica-en-los-aeropuertos.html

37 Pascual, Manuel G. (2024). La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial. El País. https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html

38 Álvarez del Vayo, M.; Bernardo, A.; Torrecillas, C. (2025). Sanidad incorpora reconocimiento facial con IA para para fichar a 170 mil pacientes de Ceuta y Melilla. Civio.es https://civio.es/sanidad/2025/07/17/sanidad-incorpora-reconocimiento-facial-con-ia-para-fichar-a-170-dot-000-pacientes-de-ceuta-y-melilla/

39 Ibid

40 Marlaska presenta la nueva "frontera inteligente" de Melilla con Marruecos tras una inversión de once millones de euros. (2025). RTVE.es https://www.rtve.es/noticias/20250205/marlaska-nueva-frontera-inteligente-melilla-marruecos/16437573.shtml#:~:text=Marlaska%20presenta%20la%20nueva%20%22frontera%20inteligente%22%20de,ten%C3%ADa%20que%20haber%20estado%20operativa%20en%202020.

41 La frontera inteligente de Ceuta ya es una realidad operativa (2025). TRC.es https://trc.es/la-frontera-inteligente-de-ceuta-ya-es-una-realidad-operativa/#:~:text=Inteligencia%20artificial%20en%20tiempo%20real,tr%C3%A1mites%20en%20el%20control%20fronterizo.

orms part of the EU's new Entry and Exit System (EES), which will affect third country nationals entering the Schengen area. **The system involves recording personal data, travel documents, fingerprints, facial images, automated document control, and high resolution cameras to monitor the border perimeter, detect suspicious activities, and enhance security in the area**[42].

This initiative has generated significant criticism from civil society and digital rights organisations. As noted in the section on legislation, despite real time facial recognition being prohibited under the AI Act for posing an unacceptable risk to the population, it may be used in border contexts under the justification of counterterrorism and national security.

Regarding the use of technologies at the border, AlgoRace, a project providing an anti racist perspective in public debates on AI, together with EuroMed Rights, published in 2024 the report Digital Technology for Migration Control at Spain's Southern Border, arguing that the use of biometric data collection tools in border contexts prioritises the detection and containment of human mobility rather than facilitating the rescue and protection of migrants, and further extends the scope of "racially discriminatory practices"[43].

**It should not be forgotten that the underlying problem with these technologies is that they are developed and implemented in a context of structural racism and therefore perpetuate historical power patterns. From an anti racist and decolonial perspective, AI technologies are observed to act as an additional mechanism of racialisation, replacing the real individual with a set of attributes evaluated as negative by the algorithm, based on biased data resulting from systemic marginalisation and criminalisation**[44].

### 3.2 Lack of Transparency and Regulatory Gaps

The cases mentioned above are only a few examples demonstrating how these systems are being regularly used in Spain for surveillance and security purposes, and at a pace and in contexts that lie beyond both the application of the AI Act and civic oversight.

In this regard, the Citizen AI Coalition (a group of organizations working to defend human rights in the context of digital technologies) states in its analysis of the final text of the Artificial Intelligence Act (AI Act) that the regulation does not sufficiently provide for citizen participation nor promote mechanisms for transparency and civic control over these technologies[45]. As an example, they note that although the regulation includes the creation of a database where AI systems must be registered, this requirement only applies to providers and implementers that are public authorities[46]. Furthermore, this database will not be publicly accessible for uses linked to security forces or in migration contexts. They also highlight that the regulation says nothing about civil society participation in fundamental rights impact assessments.

This lack of transparency in the AI Act is compounded by **the regulatory vacuum in Spain**

42 García Garrido, J. (2025). Así será la frontera inteligente de Melilla: tecnología para un paso más ágil y seguro. Telecinco.es https://www.telecinco.es/noticias/ciencia-y-tecnologia/20250224/asi-sera-frontera-inteligente-melilla-tecnologia_18_014740029.html#:~:text=La%20tecnolog%C3%ADa%20de%20la%20nueva,identidad%20m%C3%A1s%20precisa%20y%20r%C3%A1pida.&text=Adem%C3%A1s%20tambi%C3%A9n%20cuenta%20con%20un,la%20seguridad%20en%20la%20zona.

43 Ouled, Y. (2024). Algorace y EuroMed Rights presentan en el Parlamento Europeo su informe sobre la tecnología digital empleada para el control migratorio en la frontera exterior de España. Algorace.org https://www.algorace.org/2024/10/16/algorace-y-euromed-rights-presentan-en-el-parlamento-europeo-su-informe-sobre-la-tecnologia-digital-empleada-para-el-control-migratorio-en-la-frontera-exterior-de-espana/

44 Guerra, P. (2022). Algoritmos entrenados para ser racistas. Pikara Magazine. https://www.pikaramagazine.com/2022/11/algoritmos-entrenados-para-ser-racistas/

45 IA Ciudadana considera que el Reglamento de Inteligencia Artificial no ha logrado un estándar adecuado de protección de los derechos humanos (2024). IACiudadana.org https://iaciudadana.org/2024/06/18/ia-ciudadana-considera-que-el-reglamento-de-inteligencia-artificial-no-ha-logrado-un-estandar-adecuado-de-proteccion-de-los-derechos-humanos/

46 Ibid

**regarding borders and national security.** In the Spanish context, the use of biometric data such as facial recognition is regulated by the Spanish Data Protection Agency (AEPD) and the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD), but these regulations either do not address mass surveillance and border control or justify it on grounds of public security.

In 2023, the AEPD, the entity responsible for ensuring that biometric data processing complies with current data protection regulations, published its Guide on Biometric Systems for Attendance Control. The guide indicates that using biometric technologies for identification and authentication in attendance control carries a high risk due to the inclusion of sensitive data and therefore recommends the use of equivalent and less intrusive alternatives[47]. It also states that before implementing such systems, an impact assessment must be carried out demonstrating "the suitability, necessity, and proportionality of biometric data processing"[48]. Regarding the use of biometric technologies incorporating artificial intelligence, the AEPD guide establishes that these systems must consider the limitations and requirements included in the EU AI Act.

For this reason, **the AEPD guide focuses primarily on the use of biometric identification for attendance control, but does not address its use in policing, public space surveillance, or border control.**

Regarding the LOPDGDD, the law establishes that personal data may only be collected and processed under legal regulations, must adhere to the principle of data minimization (collecting only necessary data), individuals must have control over their data in terms of access, rectification, or deletion, and data processing must be transparent and secure[49]. Concerning surveillance systems, Article 22 on Video Surveillance Processing states that the processing of images via cameras may be carried out to preserve the security of people, property, and strategic facilities, and that the processing of personal data from images and sounds obtained by security forces and penitentiary centers will be governed by EU Regulation 2016/680 when the purpose is the prevention, detection, or investigation of crimes against public security[50]. In other words, we again find legislation that includes exceptions on the grounds of security.

The absence of national legislation in Spain regulating the use of facial recognition technologies in public spaces for surveillance, social control, or migration contexts from a rights-based perspective, combined with the fact that the only regulatory framework on this matter is the AI Act (with its broad national security exemption), makes the situation for fundamental rights particularly concerning. Not only will this leave the population vulnerable to arbitrary and opaque decisions by governments and security forces under the guise of national security, but the use of these technologies will also begin to automate biases, further reinforcing a system that continues to target the same social groups as always.

## 4. Impact on Fundamental Rights

### 4.1 Right to Privacy and Intimacy

First, biometric surveillance in public spaces undermines the right to privacy, considered a fundamental right in various laws and regulations, and linked to the notion of reserving for individuals a protected sphere of their personal life.

47 Guía sobre tratamiento de control de presencia mediante sistemas biométricos (2023). Agencia Española de Protección de Datos. AEPD.es www.aepd.es/documento/guia-control-presencia-biometrico-nov-2023.pdf
48 Ibid
49 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018. Boe.es https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
50 Ibid.

Article 12 of the Universal Declaration of Human Rights states that no one shall be subjected to arbitrary interference with their privacy, home, or correspondence, and that everyone has the right to legal protection against such interference[51]. Similarly, Article 8 of the European Convention on Human Rights recognizes that everyone has the right to respect for their private and family life[52]. Likewise, Article 7 of the Charter of Fundamental Rights of the European Union affirms that everyone has the right to respect for their private and family life, their home, and their communications[53]. Additionally, Article 18 of the Spanish Constitution enshrines the right to honor, personal and family privacy, and one's own image[54].

This right to privacy and personal image grants individuals the autonomy to decide what personal information they share, with whom, and for what purposes. It is a right considered fundamental to human dignity and freedom. However, the use of biometric tools in public spaces infringes upon this right to the extent that certain physical characteristics may enable the identification of groups of people without their consent and for purposes that have not been authorized by them.

### 4.2 Right to Freedom of Movement

In addition to the right to privacy and to one's own image, there is the right to freedom of movement, enshrined in Article 13 of the Universal Declaration of Human Rights[55], Article 45 of the Charter of Fundamental Rights of the European Union[56], and Article 19 of the Spanish Constitution[57] . This right can be affected by biometric surveillance to the extent that people may refrain from moving through monitored public spaces due to fear of being identified without their consent.

### 4.3 Right to Freedom of Expression and Association

From a legal perspective, a **regulatory framework that allows population control in public spaces can have a discouraging effect, causing individuals to refrain from participating in demonstrations or social debates for fear of being identified.** This is commonly referred to as the "chilling effect"[58]. Such an effect not only negatively impacts the right to assembly but can also lead to dangerous processes of social demobilization, preventing individuals from feeling safe and free to participate fully in all spheres of society and **undermining the experience of public spaces as areas for dissent and debate.**

51 Naciones Unidas (s.f.). La Declaración Universal de los Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights

52 Convenio Europeo de Derechos Humanos (s.f.). www.echr.coe.int/documents/d/echr/convention_spa#:~:text=Derecho%20al%20respeto%20a%20la,las%20libertades%20de%20los%20demo%C3%A1s.

53 Carta de los Derechos Fundamentales de la Unión Europea (s.f.). European Union Agency for Fundamental Rights. https://fra.europa.eu/es/eu-charter/article/7-respeto-de-la-vida-privada-y-familiar#:~:text=Carta%20de%20los%20Derechos%20Fundamentales%20de%20la%20Uni%C3%B3n%20Europea,-Previous%20title

54 Derechos Humanos.net Herramientas para la defensa y protección de los Derechos Humanos (s.f.). Artículo 18 de la Constitución Española. https://www.derechoshumanos.net/constitucion/articulo18CE.htm#:~:text=%2D%20Derecho%20al%20honor%2C%20a%20la%20intimidad%20personal%20y,familiar%20y%20a%20la%20propia%20imagen.

55 Naciones Unidas (s.f.). La Declaración Universal de los Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights

56 Carta de los Derechos Fundamentales de la Unión Europea (s.f.). European Union Agency for Fundamental Rights. https://fra.europa.eu/es/eu-charter/article/45-libertad-de-circulacion-y-de-residencia

57 Constitución española (1978). Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229#:~:text=25:%20%23a19%5D-,Art%C3%ADculo%2019,por%20motivos%20pol%C3%ADticos%20o%20ideol%C3%B3gicos.

58 Sánchez Barrilao, J.F. (2025). La identificación biométrica, la inteligencia artificial y el efecto desaliento en reuniones y manifestaciones. En Balaguer Callejón, F.; Escajedo San-Epifanio, L. Vigilancia biométrica masiva, Inteligencia Artificial y derechos fundamentales (pp. 527-555). Editorial Dykinson.

### 4.4 Right to Equality and Non-Discrimination

Finally, it is important to consider that biometric surveillance in public spaces does not affect all people equally. On the contrary, historically marginalized social groups may be disproportionately impacted by these technologies, such as women, LGBTIQ+ individuals and racialized people, because these tools amplify and reproduce historical patterns of power and discrimination.

## 5. Strategic Guidelines for Civil Society

The scenario described shows that biometric surveillance in public spaces is not a mere technological drift but a profound shift in the balance between power, control, and rights. Faced with the consolidation of a permissive legal framework, the expansion of opaque technologies, and the social normalization of surveillance, civil society faces a critical moment to halt democratic backsliding and demand real guarantees. For this, a forward-looking exercise is useful to anticipate possible scenarios and prepare action strategies.

In the short term (1 to 3 years), it is foreseeable that the deployment of biometric technologies in borders, airports, stations, and public spaces will increase, always under the legitimacy of the "national security" argument. Public administrations will continue promoting pilots and experimental trials in the absence of robust independent oversight mechanisms, taking advantage of legal gaps and the lack of effective accountability frameworks. At the same time, much of the population will remain unaware of the true scope of these technologies, while tech companies consolidate their role as indispensable actors in Europe's security infrastructure.

In response to these scenarios, civil society must strengthen its strategies. First, building collective power and stable coalitions is essential. Recent victories show that progress occurs when organizations work together as in Reclaim Your Face, Protect Not Surveil, or strategic litigation supported by digital rights organizations. The ability to forge transnational alliances, share legal resources, and develop common narratives will help counter the growing power asymmetry between citizens and state and corporate actors.

Second, it is imperative to demand transparency, independent oversight, and democratic control over the deployment of these technologies. This entails calling for public registers of biometric systems, fundamental rights impact assessments with community participation, independent audit mechanisms, and clear prohibitions in high-risk contexts and for policing purposes. Surveillance must stop being presented as a technical or inevitable matter and become a political and deliberative issue.

Finally, it is crucial to promote critical literacy and social counter-narratives that challenge the dominant security framework. Civil society should foster training processes aimed at activists, journalists, migrant collectives, and the general public, deconstructing the rhetoric of efficiency and technological neutrality. **Only an informed society, aware of real risks and recognizing itself as a political subject in public spaces, can resist the normalization of surveillance and mobilize to build democratic and just alternatives**.

# REFERENCES


- Álvarez del Vayo, M.; Bernardo, A.; Torrecillas, C. (2025). Sanidad incorpora reconocimiento facial con IA para para fichar a 170 mil pacientes de Ceuta y Melilla. **Civio.es** https://civio.es/sanidad/2025/07/17/sanidad-incorpora-reconocimiento-facial-con-ia-para-fichar-a-170-dot-000-pacientes-de-ceuta-y-melilla/
- Ban automated recognition of gender and sexual orientation (s.f.). All out.org https://campaigns.allout.org/ban-AGSR?_ga=2.132562957.2022005740.1643728362-441876419.1643728362
- Berthélemy, C.; Meyer, L. (2024). Tu cuerpo como pasaporte: la pesadilla biométrica en el corazón del sistema de asilo de la UE. La Marea. https://www.lamarea.com/2024/04/08/tu-cuerpo-como-pasaporte-la-pesadilla-biometrica-en-el-corazon-del-sistema-de-asilo-de-la-ue/
- Biometría: lectores de iris y escáneres de retina (s.f.). Cucorent. https://cucorent.com/blog/recursos-humanos/lectores-de-iris/#:~:text=Es%20una%20capa%20de%20tejido%20sensible%20a,extremadamente%20compleja%20y%20%C3%BAnica%20en%20cada%20individuo.
- Biurrun, A. (2022). Así es la tecnología biométrica de AENA con la que podrás coger un avión sin mostrar ninguna documentación. La Razón. https://www.larazon.es/tecnologia/20220810/fiyg44hisbfghoy6sra53l3khi.html
- Carta de los Derechos Fundamentales de la Unión Europea (s.f.). European Union Agency for Fundamental Rights. https://fra.europa.eu/es/eu-charter/article/7-respeto-de-la-vida-privada-y-familiar#:~:text=Carta%20de%20los%20Derechos%20Fundamentales%20de%20la%20Uni%C3%B3n%20Europea,-Previous%20title
- Constitución Española. (1978). Boletín Oficial del Estado. https://www.boe.es/eli/es/c/1978/12/27/(1)/con
- Control judicial de los algoritmos (2023). Asociación profesional de la magistratura (APM). Magistratura.es https://magistratura.es/control-judicial-de-los-algoritmos-_por-alfonso-peralta-gutierrez/
- Cotino Hueso, L. (s.f.). Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superppuesta de inteligencia artificial y protección de datos. Fundación Jiménez Abad. www.fundacionmgimenezabad.es/sites/default/files/Publicar/publicaciones/documentos/oc27_13_lorenzo_cotino_es_o.pdf
- Convenio Europeo de Derechos Humanos (s.f.). www.echr.coe.int/documents/d/echr/convention_spa#:~:text=Derecho%20al%20respeto%20a%20la,las%20libertades%20de%20los%20dem%C3%A1s.
- Decisión (EU) 2024/2218 del Consejo, de 28 de agosto de 2024, relativa a la firma, en nombre de la Unión Europea, del Convenio Marco el Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho. Boletín Oficial del Estado, 4 de septiembre de 2024, pp 1 a 3. https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81308
- El Parlamento Europeo refuerza el control migratorio a través de Eurodac (2022). Algorace.org https://www.algorace.org/2022/12/12/el-parlamento-europeo-refuerza-el-control-migratorio-a-traves-de-eurodac/#:~:text=Adem%C3%A1s%2C%20rebajar%C3%A1%20la%20edad%20de,a%C3%B1os%20o%20de%20por%20vida

- Escajedo San Epifanio, L. (2025). Vigilancia biométrica masiva mediante IA y derechos fundamentales: retos jurídico-constitucionales. En Balaguer Callejón, F.; Escajedo San-Epifanio, L. Vigilancia biométrica masiva, Inteligencia Artificial y derechos fundamentales (pp. 21-37). Editorial Dykinson.
- Explicación de la biometría sin contacto: métodos y aplicaciones clave (2024). Aratek. https://www.aratek.co/es/news/contactless-biometrics-explained-key-methods-and-applications#:~:text=Tecnolog%C3%ADa:%20La%20tecnolog%C3%ADa%20de%20reconocimiento%20de%20voz,almacenan%20y%20se%20comparan%20para%20su%20autenticaci%C3%B3n.
- Francia, primer país de Europa en legalizar la vigilancia biométrica (2023). La Quadrature du Net. https://www.laquadrature.net/2023/03/23/la-france-premier-pays-deurope-a-legaliser-la-surveillance-biometrique/
- Galera Victoria, A. (2025). Inteligencia artificial, biometrías y tutela de derechos a la luz del convenio marco del Consejo de Europa y la jurisprudencia del TEDH. En Balaguer Callejón, F.; Escajedo San-Epifanio, L. Vigilancia biométrica masiva, Inteligencia Artificial y derechos fundamentales (pp. 269-300). Editorial Dykinson.
- García Garrido, J. (2025). Así será la frontera inteligente de Melilla: tecnología para un paso más ágil y seguro. Telecinco.es https://www.telecinco.es/noticias/ciencia-y-tecnologia/20250224/asi-sera-frontera-inteligente-melilla-tecnologia_18_014740029.html#:~:text=La%20tecnolog%C3%ADa%20de%20la%20nueva,identidad%20m%C3%A1s%20precisa%20y%20r%C3%A1pida.&text=Adem%C3%A1s%20tambi%C3%A9n%20cuenta%20con%20un,la%20seguridad%20en%20la%20zona.
- Gibon, C. (2023). Francia quiere vigilar a las multitudes con la ayuda de inteligencia artificial y algoritmos durante los JJOO de París. Equal Times. https://www.equaltimes.org/francia-quiere-vigilar-a-las?lang=es
- Guerra, P. (2023). Por qué es importante la Ley de Inteligencia Artificial. Eldiario.es https://www.eldiario.es/opinion/tribuna-abierta/importante-ley-inteligencia-artificial_129_10602479.html
- Guerra, P. (2022). Algoritmos entrenados para ser racistas. Pikara Magazine. https://www.pikaramagazine.com/2022/11/algoritmos-entrenados-para-ser-racistas/
- Guía sobre tratamiento de control de presencia mediante sistemas biométricos (2023). Agencia Española de Protección de Datos. AEPD.es www.aepd.es/documento/guia-control-presencia-biometrico-nov-2023.pdf
- IA Ciudadana considera que el Reglamento de Inteligencia Artificial no ha logrado un estándar adecuado de protección de los derechos humanos (2024). IACiudadana.org https://iaciudadana.org/2024/06/18/ia-ciudadana-considera-que-el-reglamento-de-inteligencia-artificial-no-ha-logrado-un-estandar-adecuado-de-proteccion-de-los-derechos-humanos/
- La Ley de IA de la UE no establece un estándar de oro para los derechos humanos (2024). Edri.org https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/
- La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleado por el sector público (s.f.). Consejo para la Transparencia. Dirección de estudios / Dirección Jurídica. https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf
- La UE debe poner fin al uso de tecnología de vigilancia contra las personas migrantes y las comunidades racializadas (s.f.). Protectnotsurveil.eu https://protectnotsurveil.eu/index_es.html

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018. Boe.es https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
- Los poderosos observan a los débiles (s.f.). Reclaimyourface.eu https://reclaimyourface.eu/the-problem/
- Marlaska presenta la nueva "frontera inteligente" de Melilla con Marruecos tras una inversión de once millones de euros. (2025). RTVE.es https://www.rtve.es/noticias/20250205/marlaska-nueva-frontera-inteligente-melilla-marruecos/16437573.shtml#:~:text=Marlaska%20presenta%20la%20nueva%20%22frontera%20inteligente%22%20de,ten%C3%ADa%20que%20haber%20estado%20operativa%20en%202020.
- Naciones Unidas (s.f.). La Declaración Universal de los Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights
- Ouled, Y. (2024). Algorace y EuroMed Rights presentan en el Parlamento Europeo su informe sobre la tecnología digital empleada para el control migratorio en la frontera exterior de España. Algorace.org https://www.algorace.org/2024/10/16/algorace-y-euromed-rights-presentan-en-el-parlamento-europeo-su-informe-sobre-la-tecnologia-digital-empleada-para-el-control-migratorio-en-la-frontera-exterior-de-espana/
- Pascual, Manuel G. (2024). La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial. El País. https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html
- Permiten a una tienda sistema de reconocimiento facial para evitar a dos ladronas (2019). La Vanguardia. https://www.lavanguardia.com/vida/20190614/462862950020/permiten-a-una-tienda-sistema-de-reconocimiento-facial-para-evitar-2-ladronas.html
- ¿Qué dice la Ley europea de Inteligencia Artificial sobre los sistemas que usan datos biométricos? Algunos están completamente prohibidos y otros permitidos bajo ciertas obligaciones (2024). Maldita.es https://maldita.es/malditatecnologia/20240814/ley-ia-ue-sistemas-biometricos/
- Reconocimiento facial: Sari Real Time no cumple con las normas de privacidad (2021). Garante per la Protezione dei Dati Personali - GPDP. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842
- The role of the biometrics in the European Entry-Exit System (s.f.). Laxton. https://www.laxton.com/es/blog/the-role-of-biometrics-in-the-european-entry-exit-system/
- Tipos de sistemas biométricos: la guía completa (s.f.). Recfaces. https://recfaces.com/es/articles/tipos-de-identificacion-biometrica#:~:text=error%20de%20acceso.-,Reconocimiento%20de%20venas,en%20su%20base%20de%20datos.

# 2. EMOTION RECOGNITION AND AFFECTIVE SURVEILLANCE IN POLICING AND MIGRATION CONTEXTS

by Youssef M. Ouled

## 1. Introduction to "Emotion Recognition" Technology

If we consider the definitions provided by the Royal Spanish Academy (RAE) for the concepts of "recognition" and "emotions," both could be jointly defined as the ability to record, identify, and distinguish emotions experienced by a human being through the signals emitted by their body, such as voice or facial expressions.

In the context at hand, that of Artificial Intelligence (AI), the concept of "emotion recognition" has emerged as one of the major technological milestones, especially regarding a supposed capacity to "predict" emotions through machine learning. In this sense, "emotion recognition" technology would not only be capable of identifying, recording, and describing emotions but is also attributed with the ability to infer human emotions through the analysis of previously inputted data linked to bodily expressions.

According to the European Data Protection Supervisor, appointed by the European Commission (EC) and the European Parliament (EP), **Facial Emotion Recognition is a technology used to "analyze feelings" through images and videos.** These technologies follow the following process: face detection, facial expression detection, and classification of the emotional expression. We are referring to images that serve as input data, ranging from those captured by public surveillance cameras to those placed near advertising screens in stores, social media applications, streaming services, or personal devices.

**Referring to this technological approach inevitably involves biometrics, since we are talking about identification processes based on individual physical and behavioral characteristics that are unique to each person.** However, it is important to note that certain bodily information would not fall under the definition of biometrics for identification

purposes, yet still reveals valuable and sensitive personal data, for example, physiological signals such as heart rate, sweating, or walking rhythm. From a technological perspective, attempting to establish a relationship between changes in emotional and physiological states can identify patterns that provide information about emotional variations.

At this point, **it is worth noting that the ability to recognize emotions has been criticized as pseudoscience, as it relies on arbitrary assumptions, such as the idea that a person's internal emotions can be calibrated based on their external expressions, that is, presuming that facial expressions faithfully reflect how a person feels internally.**

Although there is no scientific support for the alleged capacity to infer emotions through technology, its proponents reference disciplines such as psychology, particularly Paul Ekman's theory of universal biological emotions, which underpins the analysis of facial expressions. This theory assumes that emotional expression and manifestation are immutable and homogeneous. Ekman's proposal establishes a series of basic and universal emotions, anger, disgust, fear, happiness, sadness, and surprise, that are "recognizable" through the analysis of facial expressions.

This represents a reductionist and ethnocentric stance that fails to consider the political implications and power asymmetries embedded in notions of the "universal," neglecting structural oppression and violence. In this line, psychologist and neuroscientist Lisa Feldman Barrett emphasizes that emotions are the result of learning conditioned by culture and prior experiences, "They are not hardwired into the brain at birth, they are constructed." Barrett highlights the implications of ignoring that emotions are shaped by context-specific and individual factors, as well as by the territory a person inhabits. These are complex variables that technological systems such as facial recognition are incapable of detecting due to the reductionism required for interpreting human interactions.

In 2016, a scientific team that included the Universidad Autónoma de Madrid analyzed how emotions are associated and identified, as well as their facial expression, in Spanish and Trobriand adolescents living in the Papua New Guinea archipelago (Oceania). This was done through two tests:

In the first, both groups of adolescents were asked to assign emotions to a set of pre-identified photographs. Comparing the results of the groups, the researchers found that, while there was consensus in associating a smile with happiness, there was no agreement for other expressions, such as neutral (without muscle movement) or in the case of a furrowed brow.

In a second phase, when asked to identify the most threatening facial expression, the Trobriand adolescents chose the one labeled "fear," while the Spanish adolescents selected the furrowed brow, labeled "anger." At the same time, the facial expression associated by the Spanish adolescents with fear and submission was identified by the Trobriand adolescents as anger and threat.

However, these are not the only criticisms leveled at "emotion recognition." Questions about its effectiveness focus on the harm it can cause regarding mass surveillance and the collection of sensitive personal data, enabling monitoring and profiling. This involves invasions of privacy, violations of rights and freedoms, and a specific impact on historically marginalized populations.

Science developed in the West has historically been shaped by a worldview that positions white and male as the norm. This logic not only conditions the context in which technological systems are implemented but also permeates the entire design and development process. Scholars such as Safiya Umoja Noble describe this by questioning the supposed neutrality and objectivity of technological systems, highlighting their role in perpetuating historical oppressions based on race and gender categories.

In this regard, sociologist and professor in the Department of African American Studies at Princeton University, Ruha Benjamin, highlights the systemic racism in which technologies such as facial and emotion recognition operate, disproportionately affecting racialized populations. This is a form of racism that is amplified and perpetuated by these technologies.

Benjamin draws a parallel between the racial segregation laws in the United States during the Jim Crow era (19th–20th centuries) and current technological systems, according to which these systems are employed to perpetuate control and repression of non-white populations. In this scenario, "emotion recognition" technologies form part of a conglomerate that establishes surveillance which profiles and criminalizes racialized populations.

In addition to the aforementioned inability to capture cultural and contextual differences, these technologies reproduce biases and errors due to the use of predominantly white faces in training datasets, which can lead to wrongful detentions in the criminal justice system and in migration control. This is documented by computer scientist and digital activist at the MIT Media Lab, Joy Buolamwini, who revealed that facial recognition systems contain gender and racial biases that increase the likelihood of errors in identifying non-white individuals, particularly Black women. This has serious consequences, such as failure to correctly identify individuals, stigmatization in public spaces such as workplaces or airports, and wrongful identification and detention of Black people categorized as criminals, with the resulting judicial consequences.

In response, Noble advocates for a technology approach grounded in greater transparency and the inclusion of profiles reflecting racial and gender diversity in the creation of these systems, aiming to minimize or reduce the risks and harms they cause. Buolamwini adds to these recommendations the need for stricter legislation governing the use of these systems. Meanwhile, Benjamin proposes an abolitionist approach to recognition technologies due to their role as an extension of policies of control and repression toward migrant and racialized populations, suggesting a reduction in their use and a reclamation of these technologies by those most affected by surveillance.

### 2. Surveillance capitalism

This is a concept extensively developed by sociologist and emeritus professor at Harvard Business School, Shoshana Zuboff, which describes an economic model in which technology companies extract personal data from all our online activity, often without the full knowledge of the individuals affected. In a scenario such as the current one, where the political and economic landscape is dominated by Big Tech companies that base their business model on the revenue obtained from mass data collection, people end up reduced to the status of products, always connected and monitored.

Ruha Benjamin adds that it is not only the mass collection of data but also the ways in which this data is collected and used to reinforce power based on racial and gender inequality. This is not a new phenomenon but continues a historical trend, as expressed by Professor Simone Browne of the University of Texas at Austin, who links the current logic of surveillance to the control and monitoring historically employed against Black populations since the era of slavery.

**Surveillance capitalism intertwines, according to Benjamin, with systemic racism that has a differential impact on non-white populations.** From limited access to digital literacy and technologies due to more precarious living conditions to hyper-surveillance focused especially on racialized communities, these are automated control tools that subtly reproduce inequality. This is evident in so-called predictive systems used in policing and the judicial system, which employ historical data reflecting institutional behavior that replicates discriminatory patterns criminalizing non-white populations. Beyond the judicial and penal spheres, this logic is present in others, such as labor and finance, where data is also used to segregate and discriminate, as mathematician Cathy O'Neil also highlights.

The use of "emotion recognition" tech is embedded within surveillance capitalism as another tool of oppression in which emotion becomes data and, therefore, information that can be interpreted, commodified, and instrumentalized by those who hold the power to do so.

This ecosystem employs updated forms of control that deny racialized individuals the capacity to control their own data and lives. To regain this control, Benjamin proposes "abolitionist tools" such as community schools with antiracist curricula, open-source software tools, community care and mutual aid networks outside state control, and the development of transparent algorithms. In other words, it is about reclaiming autonomy in the face of surveillance and data extraction.

## 3. European and Spanish regulatory framework

We can say that there is no specific law regulating "emotion recognition" technologies in Spain. Rather, this area is governed by the guidelines established under European legislation. However, as previously explained, these recognition technologies handle the recording and storage of biometric data and information, which directly impacts privacy and fundamental rights.

In Spain, the body responsible for overseeing the processing of personal data is the Spanish Data Protection Agency (AEPD), which, while not referring explicitly to emotions, requires that any data that could be used to obtain relevant personal information be treated as sensitive data (such as those related to race, ethnicity, gender, political ideology, religious beliefs, health, etc.), which are granted special protection.

In this regard, the AEPD has issued several guidelines on the use of monitoring and biometric analysis technologies that follow the principles established in the European General Data Protection Regulation (GDPR). These guidelines aim to ensure that these technologies are used in a manner respectful of personal rights and freedoms. They are especially oriented toward biometric technologies that collect and process personal data, such as facial recognition, fingerprint analysis, and voice recognition, among others. Some of the fundamental principles on which these guidelines are based include:

- **Transparency:** individuals must be clearly and comprehensively informed about what data is collected, how it is used, and for what purpose.
- **Minimization:** only data strictly necessary for a legitimate, pre-established purpose should be collected.
- **Accuracy:** data must be correct and kept up to date.

- **Storage limitation:** data must be retained only for as long as necessary to fulfill its purpose.
- **Confidentiality:** data must be protected against unauthorized access, loss, or destruction.

Following these principles, the AEPD adds that explicit consent must be obtained from the individual for their biometric data to be recorded and/or processed, and that this consent can be withdrawn at any time. In addition, individual rights are recognized, including access to processed data, its modification and deletion, as well as the right to object.

Due to the risks involved in processing such personal data, since 2018 the GDPR has made it mandatory to carry out a Data Protection Impact Assessment (DPIA) in scenarios where the processing could pose a high risk to personal rights and freedoms. This applies to technologies that use AI or algorithmic systems affecting sensitive data, or those involving profiling or mass monitoring, whether in public or private spaces. This includes biometric systems such as facial recognition. These assessments must be carried out before deployment and periodically thereafter, adapting to changes in order to identify associated risks. They must also include measures to mitigate risk and protect personal rights.

To regulate the use of AI in the EU, the European Artificial Intelligence Act, AI Act, was adopted in June 2024. Regarding the processing of personal data, it aligns with the GDPR and, in Spain, with the AEPD. The AI Act establishes a risk-based classification for AI systems.

- **Low:** systems considered not to pose a risk to rights and therefore not subject to specific requirements. This includes conventional administrative tools, such as calendar management, email handling, or virtual assistants that do not collect sensitive data.
- **Limited:** systems considered to pose a low risk to rights, requiring a minimum level of transparency regarding their operation. This includes chatbots and recommendation systems.
- **High:** systems that may impact fundamental rights, affect sensitive data, or involve profiling and potential discrimination. This category includes biometric systems capable of detecting and analyzing facial expressions, body movements, voice tone, and similar features. Their use is permitted but requires higher levels of transparency, impact assessment, and risk mitigation.
- **Unacceptable:** systems deemed dangerous to fundamental rights and freedoms, such as social scoring based on personal data or mass surveillance in public spaces without consent. Their deployment and commercialization are prohibited, although exceptions exist.

According to Article 5 of the AI Act, which sets out the basic requirements for AI systems, developers and providers of high-risk systems processing biometric data must ensure transparency in decision-making and auditability, and implement mechanisms for risk assessment and mitigation. Article 52 assigns supervisory responsibilities to competent national authorities, which in Spain are the AEPD and the Spanish AI Supervisory Agency, AESIA.

Furthermore, Article 6, Annex III, states that if a high-risk system is used for identifying individuals, even when fundamental rights are affected, it may be deployed under mandatory requirements including human oversight, a person must review automated decisions to ensure they do not negatively affect the subjects. A minimum level of transparency is also required, including logging system operation in an EU public database for high-risk systems. However, the European Council and Parliament introduced a mechanism allowing developers to determine for themselves whether their systems qualify as high-risk, meaning that if deemed otherwise, stricter transparency requirements would not apply.

## 4. Applicability and Exceptions

Despite the risks posed by the use of emotion recognition systems, it is common to find media

reports on their implementation in various sectors. Technological systems are being deployed experimentally and applied continuously, while regulatory frameworks remain slow to implement.

Examples can be found in hospitality, such as a restaurant in Aragón that uses a 360º camera to quantify the emotions detected in customers' reactions to its dishes. In culture, museums like the Thyssen-Bornemisza employ a camera, sensor, and eye-tracking system to determine which emotions are evoked when viewing paintings. In academic research, universities such as Miguel Hernández in Elche use cameras to detect gestures and emotions in faces as part of emotion recognition techniques aimed at treating autism spectrum disorders.

In recent years, there has been limited and opaque information on the implementation of these technologies in public spaces, such as transport facilities. The largest bus station in Madrid, through which thousands of people pass daily, employs a facial recognition system that automatically compares each user's face with a database of suspects and shares this information with the police, though its current application remains unclear. Renfe, the national train operator, launched a tender for video analysis software intended for deployment in stations nationwide to collect sensitive information, including ethnicity, race, and sex.

Current regulations require an impact assessment before implementing biometric data collection systems, and consultation with the AEPD is mandatory when processing poses a high risk requiring mitigation measures, as established in Article 35 of the GDPR. AEPD guidelines also recommend avoiding these systems when less invasive and less risky alternatives exist, in line with the principles of legitimate purpose, necessity, and proportionality.

Under the AI Act, Article 5 prohibits the use of biometric systems at a large scale in public or semi-public spaces, for remote or real-time identification, for classification using sensitive information, and for emotion recognition in workplaces or educational contexts, due to their invasive nature and lack of scientific basis. Exceptions do exist, however.

The regulation also bans the commercialization of systems considered unacceptable due to risks to fundamental rights and freedoms, limited to the European territory. This means that in the current context, where organizations consider Israel's actions in Palestine as genocide, the EU can still trade AI systems that violate rights and freedoms with actors being investigated by the International Criminal Court for crimes against humanity.

Research has shown that European companies develop and export surveillance and control technologies to North African countries without accountability, where they are used to repress freedom of expression and target LGBTIQ+ individuals, migrants, and racialized populations.

The AI Act also provides legal cover for activities considered "national security," allowing the use of all types of systems, including those considered high-risk or unacceptable, while offering transparency safeguards only to authorities deploying high-risk technologies, without the obligation to disclose the systems used. High-risk systems used for migration control are exempt from regulatory obligations, including those considered dangerous for EU populations, such as biometric identification, emotion recognition, fingerprint scanning, or predictive tools used to restrict migration.

These exemptions, focused on people moving from the Global South to the North, align with the recent reform of the Schengen Borders Code, the new European Pact on Migration and Asylum (PEMA), and the Eurodac update, creating an extensive technological ecosystem for mass surveillance of migrants and racialized populations, expanding state capacity to criminalize them through profiling, automatic data collection, and information sharing.

In practice, this surveillance ecosystem integrates security controls and assessments of irregular entrants to the EU, including asylum seekers. Automated decision-making systems can be applied to asylum processes, undermining the principle of individual assessment and generating less guaranteed procedures. AI systems may evaluate whether someone poses a risk to national security, public safety, or their vulnerability level without requiring justification for the final decision.

Questionable lie detectors are also being used to assess the truthfulness of asylum seekers' statements, applying biometric and emotion recognition systems to analyze facial movements and infer veracity. These systems are considered unscientific, imprecise, and risky, prohibited for EU populations but allowed for migrants and racialized individuals.

Developers justify their performance based on training with people role-playing, which researchers such as Javier Sánchez Monedero consider criminalizing. These systems operate on the presumption of dishonesty for individuals under extreme stress and vulnerability, ignoring context and individual circumstances while embedding a governance model that creates illegitimate subjects.

This governance model is mirrored in the constant surveillance applied by the Chinese government to the Uyghur population, a Muslim minority in Xinjiang, under the pretext of national security and counter-terrorism. Emotion recognition systems have been trained on this population to detect subtle facial changes and skin micro-expressions, aiming to datify lives for easier control.

Similar logic exists in the EU through repressive migration policies justified by national security and counter-terrorism. For instance, iBorderCtrl, funded by the EU for "smart border control," uses facial and emotion recognition to analyze expressions and detect "suspicious" behavior, stress, insecurity, or deception. It is applied to individuals fleeing traumatic situations who have likely endured violent migration paths. Since 2024, iBorderCtrl has been in use and evaluation at EU external borders, without precise knowledge of its functioning and impact, and without the ability for affected individuals to consent or oppose its use.

Biometric data collection requires large databases for storage and processing. Under the AI Act, while large-scale databases cannot be applied to EU populations, in migration and security contexts, massive data repositories such as ABIS, ADEXTTRA, ADPASFIL, EURODAC, and ETIAS are exempt from specific regulation until at least 2030. These databases have stored sensitive information from Global South populations for decades, exemplifying power asymmetry over people fleeing extreme situations. Data is shared with police in other EU member states and public authorities requesting access, such as tax authorities, social security, or ministries.

In addition to migration control, these databases, storing sensitive information on marginalized populations such as migrants or detainees, are used by security forces to support decision-making and train predictive algorithms for crime. These predictions are unscientific and reproduce racialized discriminatory patterns, as shown by systems such as SyRI or Sensing in the Netherlands, which target migrants and Roma populations.

Databases function as automated identification systems storing biometric information, raising significant privacy concerns, identification errors, and risks to human rights in both collection and processing. Recent investigations revealed that FRONTEX, repeatedly accused of violating migrant rights, transferred data on thousands of migrants and activists to Europol for years, obtained through interviews without guarantees to newly arrived individuals.

Data collection and analysis is not impartial but shaped by power dynamics, filtered through racial logics. UN Special Rapporteur Tendayi Achiume states that this practice is not apolitical,

particularly when powerful actors from the Global North collect information on vulnerable populations without regulated methods of oversight or accountability. This is a technology designed for mass data collection to identify, monitor, and classify people across multiple sectors, particularly migrants and racialized populations, generating criminalization, stigmatization, and discrimination, perpetuating systemic racism.

It is an invasive technology with proven inefficiency, promoting mass surveillance as an end in itself, applied without consent, and carrying enormous potential harm. Consequently, it restricts access to services and opportunities while violating rights such as privacy, data protection, and non-discrimination, and undermining fundamental freedoms, including freedom of expression.

## 5. Strategic Keys for Civil Society

In the short term, civil society must prepare for the rapid expansion of emotion recognition systems and affective surveillance technologies applied in police controls, border management, and asylum procedures. Unlike other forms of biometrics, these technologies do not only capture physical attributes but **interpret internal states,** attributing intent, honesty, or threat based on facial expressions and microgestures. This shift from identifying bodies to interpreting emotions generates far deeper risks: **it criminalizes affect, transforms stress into "suspicion," and turns vulnerability into a risk indicator.** In the coming years, pilot implementations are likely in spaces where operating without consent is easier: police interviews, asylum interrogations, automated "risk assessments," smart borders, and experimental practices justified under innovation discourses. The first strategic key is to **highlight the pseudoscientific and discriminatory nature of these technologies before they become normalized.**

In the medium term, affective surveillance will likely be integrated into the European security infrastructure as an additional layer of **automated emotional management**, particularly targeting migrant and racialized populations. The border control ecosystem is increasingly incorporating modules that classify facial expressions as "deception," "fear," "threat," or "submission." This creates a system in which emotion ceases to be a situated human experience and becomes **extractive data** used to deny rights, accelerate deportations, or justify police interventions. In response, **civil society must strengthen its monitoring and critical analysis capacity**: identify implementation patterns, record cases, demand specific impact assessments for emotion recognition, and develop narratives that reveal how these technologies amplify institutional racism.

In the long term, if no intervention occurs, these tools may consolidate a new form of political infrastructure based on the **automated interpretation of human behavior**. Affective surveillance risks becoming a permanent mechanism for classifying bodies and emotions, where control no longer operates solely over what people do but over what they supposedly feel. This has serious implications for fundamental freedoms, including mental privacy, emotional freedom of expression, and the right to seek protection without being analyzed as a "risk." It also reinforces a logic in which the emotions of some people (white, European) are seen as legitimate, while those of others (migrants, racialized) are interpreted as a threat. The long-term strategic key is to build an ethical, legal, and cultural opposition that upholds a radical idea: **emotions are not data and cannot be governed algorithmically.**

Three recommendations for civil society are therefore proposed:

**1. Publicly question the scientific and ethical legitimacy of emotion recognition.**

Promote campaigns, reports, and advocacy actions that expose its pseudoscientific nature, cultural and racial bias, and the risks of attributing intentions to people experiencing stress,

trauma, or fear. It is essential to break social acceptance of these technologies by highlighting their lack of empirical basis, demonstrated harms, and inability to interpret complex human experiences.

**2. Demand an effective prohibition in police, border, and asylum contexts, where the AI regulation allows exceptions.**

Civil society must focus pressure on spaces where these technologies are most harmful: border controls, international protection interviews, police interrogations, and high-vulnerability contexts. This involves demanding specific impact assessments, denouncing implementations, initiating litigation against unscientific uses, and pressing to close the EU exceptions invoked under "national security."

**3. Strengthen abolitionist alternatives that challenge the notion that emotions can be datified.**

Promote frameworks that recognize emotional subjectivity as a right rather than a risk; build networks of mutual support, community research, and technopolitical tools that return agency to affected people; and contest the security imaginary that turns affect into a threat. Civil society must foster a horizon in which emotion is not instrumentalized for control but protected as an inseparable part of human dignity.

# REFERENCES


- https://dle.rae.es/reconocer?m=form (reconocer + emoción)
- TechDispatch #1/2021 - Facial Emotion Recognition (European Data Protection Supervisor): https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition_en
- Crivelli, C., Russell, J. A., Jarillo, S., & Fernández-Dols, J. M. (2016). The fear gasping face as a threat display in a Melanesian society. Proceedings of the National Academy of Sciences, 113(44), 12403-12407. https://www.pnas.org/doi/full/10.1073/pnas.1611622113
- Reconocimiento de emociones: una aplicación de inteligencia artificial sin madurar que ya se usa para predecir la personalidad de la gente. (Bellio, Naiara, 2020): https://maldita.es/malditatecnologia/20210608/reconocimiento-emociones-inteligencia-artificial/
- Emotional Entanglement: China's emotion recognition market and its implications for human rights (Article 19, enero 2021): https://www.article19.org/emotion-recognition-technology-report/
- Algoritmos y desigualdad: Sistemas policiales predictivos y de perfilamiento en el ámbito judicial en España (Naiara Bellio, junio 2025): https://www.algorace.org/2025/06/11/algoritmos-y-desigualdad-sistemas-policiales-predictivos-y-de-perfilamiento-en-el-ambito-policial-y-judicial-en-espana/
- You aren't at the mercy of your emotions -- your brain creates them | Lisa Feldman Barrett (TED Talk): https://www.youtube.com/watch?v=0gks6ceq4eQ
- Emociones: ¿las sufrimos o las creamos? (Lisa Feldman Barret, marzo 2018): https://www.elperiodico.com/es/ciencia/20180313/emociones-las-sufrimos-o-las-creamos-6685845
- ¿Son universales las expresiones faciales? (Ciencia contada en español, octubre 2016): https://www.agenciasinc.es/Noticias/Son-universales-las-expresiones-faciales
- Data feminism. Cambridge: The MIT Press. (D'Ignazio, C., & Klein, L. F., 2020).
- Una introducción a la IA y la discriminación algorítmica para movimientos sociales (Valdivia, Ana y Sánchez M., Javi, 2022).
- Algorithms of Oppression: How Search Engines Reinforce Racism (Safiya Umoja Noble, 2018). Race After Technology: Abolitionist Tools for the New Jim Code (R.Benjamin, 2019).
- Gender Shades: Intersectional Accuracy Disparities in Comme
- Shoshana Zuboff: "Pensábamos que usábamos a Google, pero es Google el que nos usa a nosotros" (Justo Barranco, La Vanguardia, octubre 2020): https://www.lavanguardia.com/cultura/20201010/483967110295/shoshana-zuboff-google-facebook-trump-capitalismo-de-la-vigilancia.html
- Agencia Española de Protección del Dato: https://www.aepd.es/
- Reglamento General de Protección del Dato: https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Guía Tratamientos de control de presencia mediante sistemas biométricos (AEPD, noviembre 2023): https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf
- Guía sobre el uso de videocámaras para seguridad y otras finalidades (AEPD, noviembre 2023): https://www.aepd.es/guias/guia-videovigilancia.pdf
- Reglamento 2021/0106 (COD) del Parlamento Europeo y del Consejo sobre inteligencia artificial (AI Act): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206

- Una mesa sensorial desarrollada en Aragón ha creado el primer algoritmo que detecta las emociones de gente comiendo (María Pilar Perla, febrero 2024): https://www.heraldo.es/noticias/aragon/2024/02/20/mesa-sensorial-desarrollada-aragon-ha-creado-primer-algoritmo-deteccion-emociones-gente-comiendo-1712383.html
- El Thyssen y su experimento sobre el poder sanador del arte (RNE, marzo 2024): https://www.rtve.es/play/audios/el-gallo-que-no-cesa/gallo-no-cesa-thyssen-su-experimento-sobre-poder-sanador-del-arte/16117286/
- La UMH de Elche busca tratamiento para los trastornos del espectro autista a partir de robots sociales (David Arberola, febrero 2024): https://www.ondacero.es/emisoras/comunidad-valenciana/elche/noticias/umh-elche-busca-tratamientos-trastornos-espectro-autista-partir-robots-sociales_2024020665c1ed42c3cb3000012c04f3.html
- La mayor terminal de autobuses de España instaló reconocimiento facial en vivo en 2016, pero pocos se dieron cuenta (Naiara Bellio, agosto 2020): https://www.elsaltodiario.com/1984/autobuses-mendez-alvaro-reconocimiento-facial#
- Origen étnico, sexo o vestimenta: el polémico sistema de Renfe para vigilar a sus viajeros (Michael Mcloughlin, febrero 2021): https://www.elconfidencial.com/tecnologia/2021-02-17/renfe-videovigilancia-pliego-condiciones-tecnicos_2953824/
- Un precedente peligroso: cómo el reglamento de IA de la UE perjudica a las personas migrantes. (Marzo 2024, AlgoRace): https://www.algorace.org/2024/03/14/un-precedente-peligroso-como-el-reglamento-de-ia-de-la-ue-perjudica-a-las-personas-migrantes/
- Sobre el rumbo regulatorio de la UE en materia de tecnología y fronteras. (Febrero 2025, AlgoRace): https://www.algorace.org/2025/02/03/sobre-el-rumbo-regulatorio-de-la-ue-en-materia-de-tecnologia-y-fronteras/
- Amnistía Internacional concluye que Israel está cometiendo genocidio contra la población palestina de Gaza. (Diciembre 2024, AI): https://www.amnesty.org/es/latest/news/2024/12/amnesty-international-concludes-israel-is-committing-genocide-against-palestinians-in-gaza/
- El crimen de exterminio y actos de genocidio de Israel en Gaza. (HRW, diciembre 2024): https://www.hrw.org/es/news/2024/12/18/el-crimen-de-exterminio-y-actos-de-genocidio-de-israel-en-gaza
- Gaza: Muchas empresas se benefician con la destrucción de la vida palestina. (Julio 2025, ONU): https://news.un.org/es/story/2025/07/1540081
- Vigilancia masiva en el Maghreb y el Mashreq (Noviembre 2024, Novact, Suds, ODHE i Irídia): https://novact.org/es/publicacio/vigilancia-massiva-al-maghreb-i-al-mashreq/
- Los límites estadísticos de la vigilancia masiva: no sirve para detectar individuos sino criminalizar colectivos (Javier Sánchez Monedero, Noviembre 2019): https://www.eldiario.es/tecnologia/limites-estadisticos-vigilancia-masiva_1_1159454.html
- La frontera como base de datos (Yuly Jara, junio 2019): https://www.eldiario.es/desalambre/datos-inmigrantes-refugiados-ceden-fronteras_1_1516139.html
- Las tecnologías de automatización y el futuro de la Fortaleza Europa (Amnistía Internacional, marzo 2019): https://www.amnesty.org/es/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/
- AI emotion-detection software tested on Uyghurs (Jane Wakefield, mayo 2021): https://www.bbc.com/news/technology-57101248

- Países Bajos: Sentimos problemas: Discriminación automatizada y vigilancia masiva en la policía predictiva en los Países Bajos (Amnistía Internacional, 2021): https://www.amnesty.org/en/documents/eur35/2971/2020/en/
- EURODAC: un sistema biométrico para categorizar y criminalizar a esos migrantes y refugiados que no queremos. (Javier Sánchez M. y Ana Valdivia, abril 2022): https://www.algorace.org/2022/04/20/eurodac-un-sistema-biometrico-para-categorizar-y-criminalizar-a-esos-migrantes-y-refugiados-que-no-queremos/
- Frontex transfirió durante años ilegalmente a Europol datos de migrantes y activistas (Lola Hierro, Luděk Stavinoha y Apostolis Fotiadis, El País, 07 julio de 2025): https://elpais.com/internacional/2025-07-07/frontex-transfirio-durante-anos-ilegalmente-a-europol-datos-de-migrantes-y-activistas.html?event_log=oklogin
- ¿Quién vigila al vigilante? Violencia en las fronteras e impunidad en Frontex (Centre Delàs e Irídia, enero 2024): https://centredelas.org/publicacions/quienvigilaalvigilante/?lang=es

# CONCLUSIONS AND RECOMMENDATIONS

Public space should be, in a democratic society, a territory of freedom, inclusion, and plurality, a place where people can meet, disagree, and exercise fundamental rights without fear. However, the proliferation of surveillance technologies, from facial recognition and other forms of biometric analysis to emotion recognition systems and mass tracking of bodies and movements, is profoundly altering this condition. The expansion of these systems transforms the public sphere into an increasingly punitive, unequal environment conditioned by suspicion.

**This trend is not merely technological, it is political.** Security based on automated surveillance is not a neutral response to social problems, but an ideological construction that redefines which bodies are considered at risk, which behaviors are interpreted as deviant, and whose lives are monitored more intensively. Its effects concentrate especially on migrants, racialized communities, young people, and other groups historically subjected to control mechanisms. Rather than generating "security", these systems **erode democracy**, divert public resources toward surveillance infrastructures, and amplify structural inequalities.

Moreover, the narrative of technological inevitability, the idea that every advancement must be adopted and that innovation justifies any social cost, obscures a fundamental principle: **not all technologies are compatible with human rights.** There are democratic limits that cannot be transgressed. Some technologies, due to their design and purpose, produce structural harms that cannot be mitigated by safeguards. Recognizing these limits does not mean halting innovation, but rather orienting it toward a democratic horizon, where technology serves equality, dignity, and rights rather than undermining them. These conclusions lay the foundation for the following recommendations, aimed at guiding public policies, regulatory frameworks, business practices, and civil society actions toward genuine protection of public space as a common good.

## Recommendations for the Executive Branch and Other Political Actors

### 1. Clear prohibitions aligned with international law

- Ban biometric technologies that enable mass or discriminatory surveillance.
- Ban the development, deployment, and commercialization of emotion recognition due to inefficiency, pseudoscientific character, and documented harm.
- Prohibit systems that create or expand biometric databases by capturing images from the Internet or CCTV without legal basis or consent.
- Reject disproportionate exceptions based on national security, police action, or military needs.
- Prohibit exports of AI systems incompatible with human rights.

### 2. Democratic guarantees and limits on police use

- Ensure that any interference with privacy or data protection complies with international standards: legitimate purpose, clear legal basis, and strict necessity in a democratic society.
- Suspend or withdraw systems that do not meet standards of proportionality or transparency.
- Review contracts, pilots, and real-world trials; eliminate regulatory gaps or grey areas.

### 3. Independent assessments and binding participation

- Establish human rights impact assessment mechanisms prior to the deployment of any algorithmic system.
- Ensure binding participation of civil society, especially antiracist, migrant, and feminist movements.
- Publish all assessments, audits, datasets, and administrative decisions.

### 4. Transparency and accountability

- Create and maintain publicly accessible registries detailing all algorithmic systems used by public and private actors.
- Require registration even during pilots and real-world testing.
- Demand effective and comprehensible explainability: the public must know what system has been used, how, and with what impact.

### 5. Effective remedies and redress

- Guarantee accessible and effective complaint mechanisms for affected individuals.
- Provide judicial and non-judicial avenues for redressing rights violations.
- Protect the right of public interest organizations to represent or support affected individuals.

## Recommendations for Research Centers, Public Universities, and Private Companies

### 1. Duty of diligence and responsibility

- Implement due human rights processes throughout the lifecycle of any technological product or service, following the UN Guiding Principles.
- Prohibit the development and sale of technologies incompatible with human rights, including emotion recognition, mass biometric surveillance, and indiscriminate image capture for databases.

### 2. Impact assessments and audits

- Conduct and publish independent human rights impact assessments before any deployment.
- Implement regular external audits and verifiably correct identified risks.
- Ensure replicability, traceability, and transparency in datasets and methodologies.

### 3. Academic and technical culture committed to the public interest

- Promote independent critical research on biases, surveillance, borders, and algorithmic discrimination.
- Avoid agreements with companies that limit independence or introduce opacity.
- Avoid agreements with companies that develop technology for military or security purposes in conflict or occupied territories.
- Promote multidisciplinary teams and civil society participation in projects, especially groups sensitive to structural discrimination.

### 4. Transparency in innovation and contracting

- Ensure full transparency in contracts with the public sector.
- Publish complete technical documentation and make it accessible.
- Renounce clauses of exceptionality or trade secrecy when fundamental rights are affected or when providing services to the public sector.

## Recommendations for Journalists, Organized Civil Society, and Social Movements

### 1. Citizen oversight and counterpower

- Monitor AI deployments in the name of security and efficiency, especially at borders and in public spaces.
- Promote strategic litigation against technologies incompatible with human rights.
- Identify and denounce legal gaps, grey areas, and excessive exemptions

### 2. Rights-based journalism and narrative change

- Investigate and document harms, biases, and discriminatory practices in algorithmic systems.
- Make contracts, acquisitions, and hidden pilots visible.
- Report real impacts: exclusion, algorithmic racism, erosion of freedoms, and policing technopower.

### 3. Power building and community redress

- Ensure access to comprehensible information about systems used and their consequences.
- Support affected individuals in judicial and non-judicial claims.
- Create spaces for critical literacy on AI, algorithms, and biometric surveillance for vulnerable groups and social movements.
- Build coalitions and alliances among different movements and civil society organizations.

lafede

justícia global