European Parliament

Artificial intelligence at EU borders

Overview of applications and key issues

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Author: Costica Dumbrava
Members' Research Service
PE 690.706 – July 2021

EN

This paper provides an overview of EU initiatives on developing and deploying artificial intelligence (AI) technologies to improve border control and border security. First, it outlines the historical development of identification technologies (passport, fingerprints, photography, polygraphy, face recognition) in the social and political context. Second, it outlines the EU policy on smart borders, examining the EU's centralised information systems and major information exchange mechanisms for borders and security. Third, it surveys major EU initiatives on AI for borders by looking into four categories of AI applications: 1) biometric identification (automated fingerprint and face recognition); 2) emotion detection; 3) algorithmic risk assessment; and 4) AI tools for migration monitoring, analysis and forecasting. Fourth, it discusses key issues raised by the development and use of such AI applications, namely reliability issues (accuracy of technologies and data quality), and fundamental rights issues (bias and discrimination, data protection and security, unlawful profiling, and transparency in EU funding on AI research). The paper concludes with reflections on the broader understanding of technologies, cautioning against the pitfalls of technological determinism and the myth of technological neutrality.

AUTHOR

Costica Dumbrava, Members' Research Service

This paper has been drawn up by the Members' Research Service, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the author, please email: eprs@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, FR

Manuscript completed in June 2021

PE 690.706
ISBN: 978-92-846-8363-5
DOI:10.2861/91831
QA-08-21-191-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

The EU and its Member States are increasingly turning to artificial intelligence (AI) technologies in their efforts to strengthen border control and mitigate security risks related to cross-border terrorism and serious crime. This is a recent manifestation of a broader trend towards a 'smartening' of EU borders, a trend that also includes the development and interlinking of large-scale centralised information systems and the deployment of a decentralised information exchange mechanism for borders and security. These systems have gradually been expanded and upgraded in order to cover ever more categories of persons (that is, to close 'information gaps') and to process increasingly varied types of data (including an increased processing of biometric data).

In the course of history, states have been quick to co-opt 'new' technologies in order to solve the typically modern problem of accurately identifying individuals for the purpose of controlling mobility and tackling crime. Regardless of the sophistication and effectiveness of various identification technologies and tools (passports, body measurements, fingerprinting, photography, lie detectors or face recognition systems), their adoption has always reflected the scientific, social and political views and concerns that dominated in the relevant times and locations.

This paper identifies and discusses four major types of AI applications that the EU is using or considering using in the context of border control and border security: 1) biometric identification (automated fingerprint and face recognition); 2) emotion detection; 3) algorithmic risk assessment; and 4) AI tools for migration monitoring, analysis and forecasting.

The EU's centralised information systems for borders and security are increasingly incorporating biometric technologies for the purpose of identity verification or identification. Automated fingerprint identification technology is currently used in three information systems (the Schengen Information System, the European dactyloscopy database (Eurodac) and the Visa Information System) and will also be used in another two (the Entry/Exit System and the European Criminal Record Information System for third-Country nationals). Automated face recognition technology (FRT) is not yet used in any EU information system, but all systems except one (the European Travel Information Authorisation System) are expected to process facial images in the near future for the purpose of verification and/or identification.

Emotion detection technologies constitute one of the most controversial applications of AI at borders and elsewhere. Whereas there are currently no emotion-detection systems deployed at EU borders, a number of EU-funded projects and initiatives have explored and piloted such technologies for the purpose of enhancing border control.

Apart from verifying and identifying known persons, AI algorithms are also used to identify unknown persons of interest based on specific data-based risk profiles. Algorithmic profiling for assessing individual risks of security and irregular migration is currently being developed in the context of the Visa Information System and the European Travel Information Authorisation System. Automated, intelligence-driven risk assessment is carried out by Member States in the framework of the exchange of passenger data among them.

The EU is also investing in AI-based tools for monitoring, analysing and forecasting migration trends and security threats. The European Asylum Support Office is currently using an early warning and forecasting system to predict the number of asylum applications. The European Commission and the EU agencies in the area of freedom, security and justice are exploring other applications in this field, including in the context of the development of the Frontex EUROSUR system and the Europol innovation hub.

There are clear benefits to be reaped from a careful adoption of AI technologies in the context of border control, such as increased capacity to detect fraud and abuses, better and timely access to relevant information for taking decisions, and enhanced protection of vulnerable people. However, these benefits need to be balanced against the significant risks posed by these technologies to fundamental rights.

Despite progress regarding biometric identification technologies, the accuracy of the results still varies across technologies and depends on contextual factors. Even the relatively well-established fingerprint identification applications face challenges, in particular at the stage of the collection of biometric data (related to, for example, subjects' age and environmental conditions). The reliability of face recognition technologies in 'real world' settings is highly dependent on the quality of the images captured and on the quality of the algorithms used for biometric matching. The quality of the algorithms depends, in turn, on the quality of the training datasets (including the quality, completeness and relevance of training images) and the various optimisation techniques. Serious doubts exist about the scientific basis and reliability of emotion-detection algorithms. Concerns about data accuracy have been raised with regard to many EU information systems and information exchange frameworks for borders and security.

Face recognition technologies have come under increased scrutiny due to concerns about fundamental rights, in particular risks related to bias and discrimination, data protection and mass surveillance. Whereas great attention has been paid to the issue of bias and discrimination, it must be noted that even accurate and unbiased AI systems may pose significant other risks, including to data protection and privacy. The increased use of biometric data in EU information systems amplifies the risk of unlawful profiling (for example, facial images may reveal ethnic origin). Even when profiling is not based on biometric or personal data, other types of data or combinations thereof used for algorithmic profiling may lead to discrimination based on prohibited grounds. Existing safeguards, such as the human-in-the-loop safeguard (requiring human interaction) and the right to explanation may not be sufficient to tackle these risks. As transpired in the case of an EU-funded research project focused on developing emotion-detection technologies, there is a need to enhance the transparency and oversight of EU funding on AI research, in particular in highly consequential areas such as borders and security.

Finally, the development and adoption of powerful AI technologies would benefit from a full understanding of and reflection on broader aspects, including the historical roots of technologies and the prevailing social and political views and expectations. Adopting technologies without confronting pitfalls such as technological determinism and the myth of technological neutrality would further weaken fundamental rights, transparency and accountability.

Table of contents

Table of figures

Table of tables

List of main acronyms used

ABC:	automated border control
AFIS:	Automated Fingerprint Identification System
AI:	artificial intelligence
API:	advance passenger information
CIR:	Common Identity Repository (interoperability component)
EASO:	European Asylum Support Office
ECJ:	Court of Justice of the European Union
ECRIS-TCN:	European Criminal Record Information System for Third Country Nationals
EES:	Entry-Exit System
EIBM:	European integrated border management
EPS:	European search portal (interoperability component)
ETIAS:	European Travel Information Authorisation System
eu-LISA:	Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurodac:	European dactyloscopy database
Europol:	European Union Agency for Law Enforcement Cooperation
EUROSUR:	European Border Surveillance System
FRA:	EU Agency for Fundamental Rights
Frontex:	European Border and Coast Guard Agency
GDPR:	General Data Protection Regulation
iBorderCtrl:	Intelligent Portable Control System
JRC:	European Commission Joint Research Centre
LED:	Law Enforcement Directive
MID:	multiple identity detector (interoperability component)
MRTD:	machine-readable travel documents
PNR:	passenger name records
sBMS:	shared Biometric Matching Service (interoperability component)
SIS:	Schengen Information System
VIS:	Visa Information System

1. Background information on identification technologies

Fixed physical borders, as demarcated by brick-and-mortar walls or barbed wire fences, are a powerful symbol of sovereign control over a territory. Despite constant efforts to erect and reinforce physical borders (such as walls and barriers[1]), border control is increasingly shifting both within and beyond a delineated territory.[2] The extension of control beyond the actual site of the border is realised through a number of 'remote control' strategies,[3] such as pre-departure registration, remote checks and digital surveillance. The inward and outward shifting of borders is supported by a number of border technologies for biometric identification, profiling and risk analysis.

1.1. Identifying mobile and risky people

From a historical perspective, the approaches used to identify persons within a territory emerged in response to the growing need of the modern state to know its people[4] in order to govern large and increasingly mobile populations. The problem of identification became particularly acute in the wake of the Industrial Revolution, when increased mobility (both internal and external) transformed local communities into 'societies of strangers', filled with mobile and potentially dangerous people.[5]

Techniques that made it possible to uniquely and unambiguously identify each person developed gradually, building on previous disparate practices (such as travel passes) aimed in particular at enabling the mobility of the few (merchants, diplomatic envoys) and controlling the mobility of the many (the poor and 'dangerous classes'). The invention of the (national) passport following the French Revolution was also meant to primarily regulate the internal movement of people.[6] However, the gradual adoption of passports served to establish better control at borders and to clearly distinguish between those entitled to enter a country (citizens) and those who required special authorisation (non-citizens). Moreover, passports were also used to control exit, so as to either enable or restrict emigration.

Being low-level border technologies, passports and other documentary evidence (e.g. visas) lent themselves easily to abuse (they could be forged or passed from one person to another) and, until the establishment of specific border institutions and infrastructure, passport checks and border control could not be systematically enforced. One of the key challenges was verifying the authenticity of documents and establishing a traveller's identity. Whereas some documents included physical descriptions of the persons, these were usually generic and subjective.

While national passports became generalised before the First World War, significant efforts to standardise passports accelerated after the Second World War. The International Civil Aviation Organization (ICAO), established in 1944, has played a key role in establishing standards for travel

---

1 A. R. Benedicto, M. Akkerman, and P. Brunet, A Walled World: Towards a global apartheid, report, Transnational Institute (TNI), 18 November 2020.

2 A. Shachar, 'Borders in the Time of COVID-19', Ethics and International Affairs, online blog, March 2020.

3 A. R. Zolberg, 'Managing a world on the move. Population and Development Review', *Population and Development Review*, 32, 2006.

4 James C. Scott, *Seeing like a state: How certain schemes to improve the human condition have failed*, Yale University Press, 2008.

5 S. A. Cole, *Suspect identities: A history of fingerprinting and criminal investigation*, Harvard University Press, 2001.

6 J. C. Torpey, *The invention of the passport: Surveillance, citizenship and the state*, Cambridge University Press, 2008.

documents. For example, in 2005 the ICAO member states[7] approved a new standard requiring all states to issue, as of 2020, machine-readable travel documents (MRTD).[8]

Other attempts to solve the problem of identification took place in the context of criminal justice, the aim being to recognise and keep track of multiple offenders (recidivists). Anthropometry, the science of measuring human bodies, offered a promising method to assign a stable identity to persons. The most famous anthropometric system was developed by the French police official Alphonse Bertillon in the late 1870s. Bertillon sought to collect a series of precise measures and descriptions of a convict's body in order to record his or her identity, classify the information and store it on file for later comparisons.[9] By the end of the 19th century, the 'Bertillonage system' (or versions of it) had been adopted by many countries in Europe and beyond.

1.2. The discovery of fingerprints

Whereas some evidence suggests that fingerprints were associated with individual identity as early as 4 000 years ago, the first identification systems based on a systematic and standardised collection and interpretation of fingerprints were developed in the late 19th century William Herschel, a British colonial administrator in India, used inked impressions of a hand and later of the tips of the fingers as a method to prevent fraud and misrepresentation in delivering civil contracts and collecting government pensions. Physician Henry Faulds, another British colonial, proposed a classification system to sort and search fingerprints that could be used to establish a criminal investigation register.[10] It was nevertheless Francis Galton, a scientist and Charles Darwin's cousin, who developed a system of fingerprint analysis based on 'minutiae' features ('Galton points'), which laid the foundation of the science of fingerprint identification.

In the beginning of the 20th century, anthropometry was gradually replaced by fingerprinting as the ultimate marks of unique identities (even Bertillon added fingerprints to his identification cards). While fingerprinting became a common criminal investigation practice, it also attracted interest from officials dealing with mobility and migration control. For example, a 1912 law in France obliged itinerant persons to carry a '*carnet des nomades*', which included fingerprints and photographs.[11]

In the US, in the context of mounting restrictions on Chinese immigration at the end of the 19th century, fingerprinting was proposed as a method of identifying Asian individuals (although, in the end, it was decided to use photographs instead).[12] The idea of using fingerprints for identifying foreigners took off in Argentina, where the development of an alternative fingerprint classification system ('dactyloscopy') by criminologist Juan Vucetich coincided with public concern about overwhelming immigration of people of an 'inferior' racial background.[13]

Traditionally, fingerprints were taken in sets of 10, using ink and paper. The accuracy and practicability of pre-digital biometric identification methods depended heavily on the amount of information on record and the operator's capacity to (manually) retrieve the relevant files and to match information. The usefulness of fingerprints also relied on the existence of systems to exchange and link fingerprint

7 All EU Member States are part of the ICAO, and the EU is an ad-hoc observer.

8 MRTD display information and biometric traits that identify a person and contain an embedded machine-readable chip storing biographic and biometric information about the person.

9 Cole, 'Suspect identities', 2001, pp. 32-59.

10 ibid., pp. 64-75.

11 Torpey, *The invention*, 2008, p. 132.

12 Cole, *Suspect identities*, 2001, p. 126.

13 ibid., pp. 128-133.

records at national and international level. Early efforts to establish centralised international criminal records resulted in the establishment of the Bureau for Distant identification in Copenhagen (in 1922) and the International Criminal Police Congress (in 1923), the predecessor of Interpol.

1.3. The face of crime

Photographs have been used to identify people since the invention of photography (primitive facsimile technology was used as early as 1843). Faces of know criminals ('rogues' galleries') started to be displayed publicly or circulated among authorities as early as the 1850s, first in the US and later in Europe.[14] Whereas photographs of faces could intuitively represent individuals, their reliability and practicability for identifying people was limited. A key obstacle was the absence of a system for cataloguing or indexing images for later search and retrieval. Bertillon included facial photographs in his cards (thus inventing the 'mug shot' – a police photograph of a person taken after they have been arrested), but only as an additional element.

Anthropometric efforts to identify people have been mixed with attempts to find a physical cause of criminality, demonstrate racial hierarchies and justify eugenic interventions in society.[15] For example, adepts of the study of physiognomy (made extremely popular in 18th century Europe by a Swiss cleric, Johann Kaspar Lavater) sought to deduce one's personality and character from their outer appearance, especially the face. The appeal of physiognomy persisted long after it had been scientifically refuted.[16]

Photographs were also hoped to provide a window into a person's inner life and dispositions. The new technology gave new life to criminal physiognomy. Francis Galton, for example, built composite photographs by superimposing photographs of convicts (men) in search for a pictorial representation of a paradigmatic criminal face.[17] Lavater and Galton believed that physiognomy could serve as 'a tool to better humanity', thus providing legitimacy to the eugenic movement of the 20th century.

1.4. Mind-reading machines

Recent enthusiasm about all-powerful artificial intelligence has rekindled century-old hopes and claims about machines that catch liars, read people's minds and detect criminal intent. Facial expression recognition technologies are currently developed or adopted for the purpose of detecting human emotions and mental states, for example, to assess whether people are lying or telling the truth.[18] As is the case with most biometric technologies, border management constitutes a key domain for experimenting with emotion detection technologies.[19]

Early attempts to build machines for detecting criminal intentions ('criminal dangerousness') date back to the 1880s and included 'pneumographs' (measuring variations in breathing) and 'sphygmographs' (measuring blood pressure).[20] These attempts culminated in the 1920s with the

---

14 Cole, *Suspect identities*, 2001, p. 20.

15 B. Agüera y Arcas et al., Physiognomy's New Clothes, medium.com, May 2017.

16 A. Todorov, *Face value: The irresistible influence of first impressions*, Princeton University Press, 2017.

17 S. Chinoy, The Racist History Behind Facial Recognition, *New York Times*, 10 July 2019.

18 L. van Woensel and N. Nevil, What if your emotions were tracked to spy on you?, At a Glance, EPRS, European Parliament, March 2019.

19 K. A Gates, *Our biometric future: Facial recognition technology and the culture of surveillance*, New York University Press, 2011.

20 G. C. Bunn, *The truth machine: A social history of the lie detector*, John Hopkins University Press, 2012.

building of the first polygraph (lie detector), able to record and interpret several physiological indicators such as blood pressure, pulse, respiration and skin conductivity. Despite inconsistent results and the high stakes involved, the lie detector remained an accepted interrogative device in criminal investigations until the end of the 20th century. In the US, it was used by the FBI and the military until 1998, when the US Supreme Court concluded that 'there was simply no consensus that polygraph evidence is reliable'.[21] The polygraph is still used today for some other purposes, such as post-offence monitoring of sex- and other violent offenders in the US and the UK.[22] Despite serious doubts about the reliability of the polygraph, new technologies are reigniting researchers' hopes of reading the mind by measuring the body. Apart from using face recognition technologies, they are applying alternative approaches that rely on functional magnetic resonance imaging technology, electroencephalography, eye-tracking, voice analysis or thermal facial analysis.[23]

1.5. Automated identification and artificial intelligence

In the pre-digital era, the collection, verification and classification of biometric markers was done by humans (aided by non-digital technologies). This often implied a labour-intensive process, and the accuracy of the results varied according to the training and diligence of the operators and the administrative systems in place. Digital technologies made it possible to automate both the enrolment (the capture of images) and the analysis of biometric markers, which led to the development of specialised IT systems (databases) and network infrastructure.

While the first attempts to automate fingerprint identification date back to the 1940s (using IBM punch cards to retrieve fingerprint records), fully automatic fingerprint identification systems (AFIS) developed from the 1960s onwards. With the development of optical scanners in the late 1980s, it became possible to scan images of fingerprints directly into a computer.[24] While automated fingerprint identification systems have become widely integrated in border management, a number of other biometric technologies are currently being developed and tested, including facial image recognition, iris recognition and DNA profiling.

Recent advances in artificial intelligence (AI) technologies have led to a surge of applications based on face recognition. Apart from becoming a convenience for consumers, used to tag photos on social media, unlock devices, and access homes and bank accounts, facial recognition technologies provide highly sought-after capabilities for criminal identification and public surveillance.

In the context of borders, it is argued that 'facial recognition technologies are transforming ports of entry and exit into true panopticons, tracking and identifying travellers at numerous points throughout their border control journey and linking identification points that were previously distinct'.[25] Besides automated identification, AI applications are increasingly adopted in the areas of

[21] K. Crowford, 'Time to regulate AI that interprets human emotions', *Nature*, 6 April 2021.

[22] M. Oswald, 'Technologies in the twilight zone: early lie detectors, machine learning and reformist legal realism', *International Review of Law, Computers & Technology*, 34(2), 2020.

[23] J. Sánchez-Monedero and L. Dencik, 'The politics of deceptive borders: "biomarkers of deceit" and the case of iBorderCtrl', *Information, Communication & Society*, 2020.

[24] Cole, *Suspect identities*, 2001, pp. 250-258.

[25] T. Israel, 'Facial recognition at a crossroads: Transformation at our borders and beyond', Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), September 2020, p. iv.

borders, migration and security for a variety of purposes, including for emotion detection, individual risk assessment, migration monitoring and analysis, and decision support systems in immigration.[26]

2. EU smart borders

2.1. IT systems and information exchange

The establishment of the Schengen area as a space with no internal borders was accompanied by the gradual development of EU policies on external borders, including common rules on border control, an EU visa and police cooperation. A key element of these policies has been the development and expansion of IT systems and information exchange mechanisms supporting border management and law enforcement cooperation.

After the establishment, between 1995 and 2004 of the first generation of EU information systems for asylum, visa and border management, in 2008, the Commission proposed to establish two new systems: an entry/exit registration system and an electronic system of travel authorisation.[27] The two proposals formed the smart borders package, which was put forward in 2013.[28] However, the package met with wide criticism (in particular regarding its feasibility) and the co-legislators could not reach agreement.

Following the 2015 migration crisis and in line with the European agenda on migration,[29] in April 2016 the Commission published a communication on stronger and smarter information systems proposing to 'strengthen and improve [the EU's] IT systems, data architecture and information exchange' in order to cover the 'existing information gaps'.[30] This was followed by a number of legislative proposals to expand existing systems, create new ones and establish interoperability.

2.1.1. Overview of EU information systems and recent developments

The Schengen Information System (SIS)[31] was established in 1995 and updated in 2013 and again in 2018. The SIS enables the competent authorities to access it and to consult alerts for the purpose of refusing entry into or stay in the Schengen area, or to consult alerts on missing persons and on persons or objects related to criminal offences. An update of the SIS legal framework in 2018[32] introduced new categories of alerts (on unknown suspects or wanted persons, on children at risk of parental abduction, on entry bans, and on persons ordered to return). It also allowed the processing of more types of data, including new biometric data (palm prints, facial images and DNA profiles related to missing persons). The new SIS features are expected to become fully operational in December 2021.

The European dactyloscopy database (Eurodac)[33] was established in 2000 and became operational in 2003. Eurodac supports the implementation of EU asylum legislation by establishing

---

26 P. Molnar and L. Gill, 'Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System', University of Toronto and the Citizen Lab, 2018.

27 European Commission, communication on Preparing the next steps in border management in the European Union, February 2008.

28 European Commission, Smart borders – background, Migration and Home Affairs.

29 European Commission, communication on A European Agenda on migration, May 2015.

30 European Commission, communication on Stronger and Smarter Information Systems for Borders and Security, April 2016.

31 European Commission, Schengen Information System, Migration and Home Affairs.

32 European Parliament, The revision of the Schengen Information System II, Legislative Train Schedule.

33 European Commission, Identification of applicants (Eurodac), Migration and Home Affairs.

the point of entry into the EU of persons seeking international protection in order to help determine the country responsible for examining their applications. Under certain conditions, law enforcement authorities can access the system to prevent, detect and investigate terrorist offences and other serious crimes. Building on discussions around a 2016 proposal[34] to update Eurodac, in September 2020 the Commission presented an amended proposal[35] as part of the new migration and asylum package. Overall, the main changes concern: collecting alphanumerical identity data to enable the counting of applicants (not just applications); including new categories of persons (persons disembarked following search and rescue operations); processing new biometric data (facial image); and lowering the age for fingerprinting (from 14 to 6 years). The amended proposal is currently under examination by the co-legislators.

The Visa Information System (VIS)[36] was established in 2004 and became operational in 2011. The VIS contains information about applications for short-stay (Schengen) visas. It enables border guards to verify that a person presenting a visa is its rightful holder and to identify persons within Schengen territory who have fraudulent or no documents. Under certain conditions, national authorities and Europol can access VIS data for the purposes of preventing, detecting and investigating terrorist and criminal offences. In 2018, the Commission presented a proposal[37] to update the VIS with a view to expanding its scope (include data on long-stay visas and residence permits) and enhancing checks in visa processing (enabling background checks to identify risks). The VIS is also expected to assist with identifying and returning any person who no longer fulfils the conditions for entry to, stay or residence in the Member States. The Parliament adopted its legislative resolution[38] on the proposal in March 2019. Following agreement in trilogue negotiations, the Council adopted the revised regulation on 27 May, with the Parliament completing its second reading in July 2021.

The Entry/Exit System (EES)[39] was established in 2017 and is expected to become operational in 2022. The EES will allow to digitally record the entry and exit (and refusal of entry) of short-stay visa-holders and visa-exempt travellers who cross the EU's external borders. It will automatically calculate the duration of a person's authorised stay (accessible via a website), and generate alerts to Member States when the authorised stay has expired. Under certain conditions, law enforcement authorities and Europol will be able to access the EES for preventing, detecting and investigating terrorist offences or other serious crimes.

The European Travel Information Authorisation System (ETIAS)[40] was established in 2018 and is expected to become operational in 2022. ETIAS will allow for the pre-registration of visa-exempt visitors travelling to the Schengen area and for assessing security or irregular migratory risks posed by these persons before they arrive at the border. ETIAS will also establish a watchlist of persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on

---

34 European Commission, Proposal for a Regulation on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013, May 2016.

35 European Commission, Amended proposal for a Regulation on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX, September 2020.

36 European Commission, Visa Information System (VIS), Migration and Home Affairs.

37 European Commission, Proposal for a Regulation amending Regulation (EC) No 767/2008, May 2018.

38 European Parliament, Legislative resolution of 13 March 2019 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008.

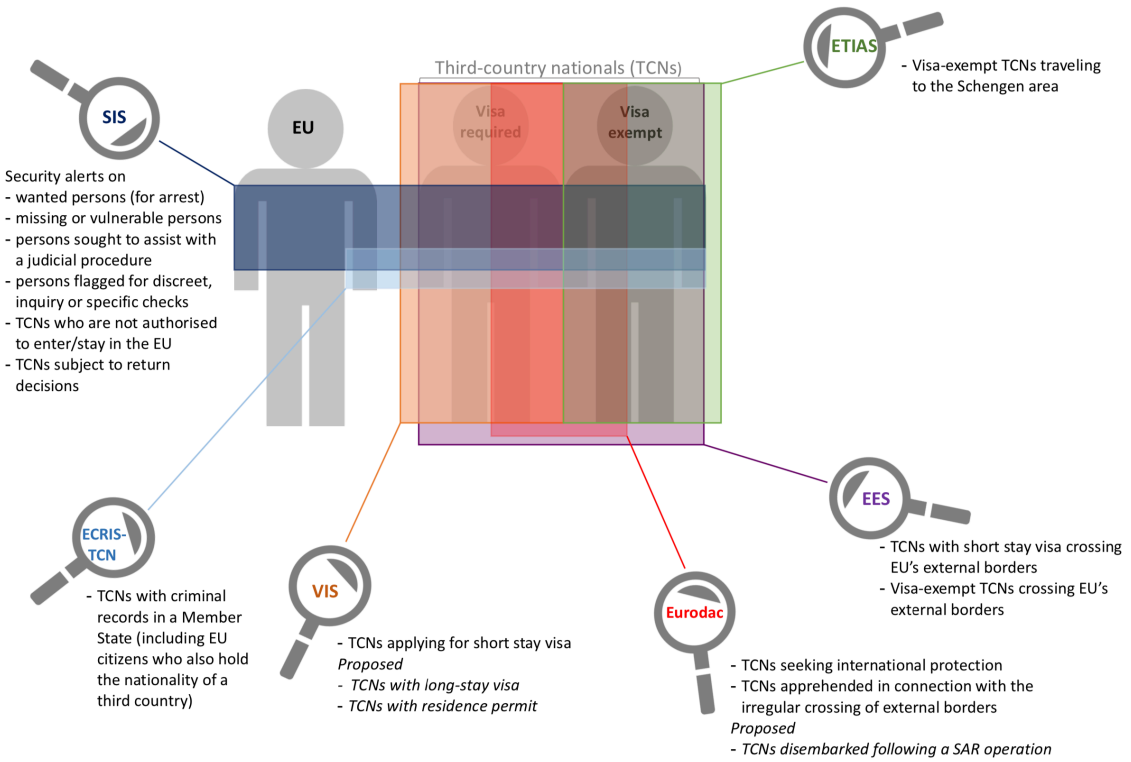
39 European Commission, Entry/Exit System (EES), Migration and Home Affairs.

40 European Commission, European Travel Information and Authorisation System (ETIAS), Migration and Home Affairs.

an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence.

The European Criminal Record Information System for third-country nationals (ECRIS-TCN)[41] was established in 2019 and is expected to become operational in 2022. ECRIS-TCN will make it possible to ascertain which other Member States hold criminal records on third-country nationals or stateless persons, or EU citizens who also hold the nationality of a third country. The inclusion of the latter category has raised concerns about creating 'second-class' EU citizens.[42]

Figure 1: Overview of the European information systems for borders and security



Source: Author's compilation from publicly available sources.

2.1.2. Interoperability of information systems

Regulations (EU) 2019/817 and (EU) 2019/818 established interoperability rules between the European information systems in the field of borders and visa and in the field of police and judicial cooperation, asylum and migration, respectively. A key aim is to facilitate the correct identification of persons, including unknown persons, persons who are unable to identify themselves, and unidentified human remains. Interoperability covers the three existing centralised systems (SIS, VIS and Eurodac), and the three systems under development (EES, ETIAS, and ECRIS-TCN). Regulation (EU) 2017/2226 (the EES Regulation) requires the establishment of interoperability between the EES

41 European Commission, European Criminal Records Information System (ECRIS).

42 Meijers Committee, 'Creating second-class Union citizenship? Unequal treatment of Union citizens with dual nationality in ECRIS-TCN and the prohibition of discrimination', n.d.

and the VIS by providing a direct communication channel between the two systems. Interoperability should enable direct consultations from the VIS to the EES and vice versa.

The implementation of interoperability requires developing technical infrastructure at the central (EU) and the national levels. The technical work is carried out by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). The mandate of eu-LISA was revised in 2018 to reflect the agency's new roles in developing and managing EU information systems, including their interoperability.

Interoperability components

The interoperability regulations provide for four main interoperability components:

- The **European search portal** (ESP) will allow competent authorities to search multiple systems using both biographical and biometric data. The ESP will enable the simultaneous querying of the EU centralised systems, the Europol information system and the Interpol system.
- The **shared biometric matching service** (sBMS) will facilitate the identification of an individual who is registered in the SIS, Eurodac, the VIS, the EES, and ECRIS-TCN. The sBSM will store biometric templates (not the actual data) from the systems (logically separated) in one single location and will facilitate cross-system comparisons using biometric templates.
- The **common identity repository** (CIR) will facilitate the correct identification of persons by establishing individual files containing alphanumerical identity data, biometric data, and travel document data of all individuals registered in the EES, the VIS, ETIAS, Eurodac and ECRIS-TCN.
- The **multiple identity detector** (MID) will create and store links between data in the different systems in order to detect incorrect, incomplete or fraudulent identity data or travel document data.

The full implementation of interoperability also depends on the adoption of relevant legislative acts (such as the VIS and Eurodac proposals) and specific delegated and implementing acts. The Commission has started designing the necessary implementing measures. In its August 2020 report[43] on the state of play of interoperability, the Commission assessed that work was on track, but expressed concerns about certain elements (e.g. the development of the EES's national components) and contemplated the possibility of delays arising from the impacts of the Covid-19 crisis. According to a Commission note[44] of 1 June 2021, 'some Member States still face considerable risks of delays' in the implementation of the EES and the updated SIS, mainly due to delayed procurement procedures.

2.2. European integrated border management

The EU has been gradually developing a European integrated border management (EIBM) system to enable national and European coordination and cooperation in the area of border management. Two recent regulations (Regulation (EU) 2016/1624 and Regulation (EU) 2019/1896) established the European Border and Coast Guard as a shared responsibility of the European Border and Coast Guard Agency (Frontex) and the national authorities responsible for border management, and defined the scope and framework of EIBM. The update also provided for the creation at Frontex of a standing corps of up to 10 000 operational staff by 2027.

[43] European Commission, Report on the state of play, 2020.

[44] European Commission, Implementation of interoperability: state of play on the implementation of the Entry/Exit System and the European Travel Information and Authorisation System, 2021

2.2.1. Components of EIBM

EIBM is based on a four-tier-access control model comprising measures concerning not only controls and operations at the external borders but also measures beyond the external borders (such as information exchange and training activities in neighbouring countries and in countries of origin and transit of irregular migration) and within the Schengen area (e.g. police cooperation, risk analysis and return operations). There are 11 EIBM components:

- border control;
- search and rescue;
- cooperation among relevant EU institutions, bodies, offices and agencies;
- cooperation with third countries;
- technical and operational measures within the Schengen area;
- return of third-country nationals;
- state-of-the-art technology and information systems;
- quality control mechanism;
- solidarity mechanisms.

In 2019, Frontex published the technical and operational strategy for EIBM,[45] which defined several strategic objectives, including sustaining European border and coast guard capabilities by, among others, identifying and exploiting state-of the art technology. The strategy advocated a 'knowledge-based border control' that relies increasingly on pre-arrival information and makes effective use of all relevant information systems. The first policy document for the multiannual strategic policy and implementation cycle is expected to be finalised in the first half of 2021.

2.2.2. European Border Surveillance System

The European Border Surveillance System (EUROSUR)[46] was established in 2013 and became operational in 2014. EUROSUR is a framework for information exchange and cooperation between the Member States and Frontex, aiming to improve the detection, prevention and combating of illegal immigration and cross-border crime at the EU external borders. EUROSUR is managed by Frontex and covers land, maritime and air border surveillance (including on pre-frontier areas), as well as checks at border crossing points, border operations and integrated planning. EUROSUR's communication network is currently updated and is expected to become fully operational in 2025.

EUROSUR follows an intelligence- and risk analysis-driven approach and is instrumental for establishing national and European situational pictures at borders, carrying out risk analysis and supporting reaction capabilities. A situational picture is defined as 'an aggregation of geo-referenced near-real-time data and information received from different authorities, sensors, platforms and other sources'.

The EUROSUR Fusion Services provide analyses on the external borders that can be based on a variety of activities, including: selective monitoring of designated third-country ports and coasts and of designated pre-frontier areas; tracking of suspect vessels and aircraft; monitoring of migratory flows towards and within the EU in terms of trends, volume and routes; media monitoring, open source intelligence and analysis of internet activities; and analysis of information derived from large-scale information systems for the purpose of detecting changing routes and methods used for illegal immigration and cross-border crime.

---

45 Frontex, Technical and Operational Strategy for European Integrated Border Management, May 2019.

46 European Commission, EUROSUR, Migration and Home Affairs.

Frontex is tasked with preparing general annual risk analyses and strategic risk analyses (based on anonymised data and following a common integrated risk analysis model) covering all aspects relevant to EIBM and with a view to developing a pre-warning mechanism. Frontex also prepares vulnerability assessments regarding the capacity and readiness of Member States to face present and upcoming challenges at the EU external borders.

2.3. Probing artificial intelligence for EU borders

The Commission and the EU agencies are actively exploring opportunities offered by AI in the area of border management, migration and security. In 2020, the Commission established an Expert Group on Artificial Intelligence in the domain of Home Affairs[47] to help in the preparation of legislative proposals and policy initiatives related to AI.

A 2020 study[48] for the Commission identified five clusters of opportunities for the use of AI in border control, migration and security: chatbots and virtual assistants; risk assessment and application triaging in the context of the visa process; knowledge management tools; policy insight and analytics tools; and computer vision applications 'to gain insights from image processing of individuals (faces, fingerprints, etc.) and objects'. Other studies for the Commission explored the possibility of developing a forecasting and early warning tool for migration based on AI technology,[49] and the possibilities for the development of data spaces (frameworks for data sharing) for law enforcement.[50] While doing its preparatory work ahead of making its 2021 proposal on an AI regulation, the Commission requested a study[51] to support an impact assessment of the regulatory requirements for AI in Europe. In its new Schengen strategy,[52] presented in June 2021, the Commission restated the need to make the best use of existing and future technologies in border management. It also underlined the importance of developing and deploying AI technologies for law enforcement.

In a 2020 report,[53] eu-LISA presented its approach to AI, which focuses on i) supporting the necessary computational infrastructure for the development and testing of AI tools for the key stakeholders, and ii) developing AI solutions in the area of performance monitoring, service management, virtual assistants, cybersecurity, and energy performance. These applications are deemed by the agency to raise limited ethical and legal considerations or none.

In 2021, Frontex published a study[54] mapping AI technologies and capabilities for border security. The study identified a number of promising AI applications for automated border control and border surveillance.

---

47 European Commission, Commission Expert Group on Artificial Intelligence in the domain of Home Affairs.

48 Deloitte, 'Opportunities and challenges for the use of artificial intelligence in border control, migration and security', May 2020.

49 Ecorys, Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology, November 2020.

50 M. J. Flynn, 'Study on technical requirements for data spaces in law enforcement', June 2020.

51 A. Renda, J. Arroyo, R. Fanni, M. Laurer, A. Sipiczki, T. Yeung, G. Maridis, M. Fernandes, G. Endrodi, S. Milio, V. Devenyi, S. Georgiev and G. de Pierrefeu, 'Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe', April 2021.

52 European Commission, Communication on a strategy towards a fully functioning and resilient Schengen area, June 2020.

53 eu-LISA, Artificial Intelligence in the Operational Management of Large-scale IT Systems, July 2020.

54 Frontex, Artificial Intelligence - based capabilities for European Border and Coast Guard, March 2021.

3. Automated biometric systems

Automated biometric systems can be used for two main purposes:

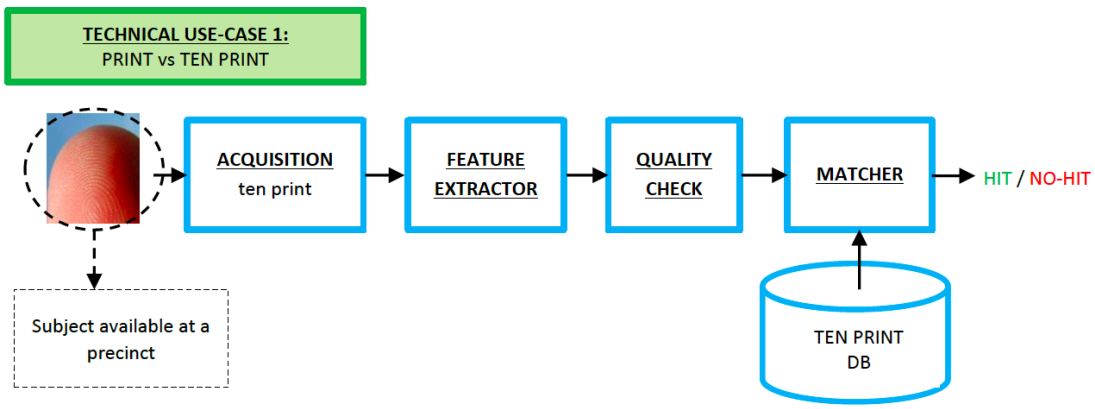
1. **Biometric verification** (or authentication) of identity, where a biometric image (fingerprint or facial image) is captured and compared to an image stored on a biometric travel document or in a database (one-to-one matching).
2. **Biometric identification**, where a biometric image is matched against other images stored in a database (one-to-many matching). A closed-set identification is when the subject's data is known to be in the reference database, whereas an open-set identification is when it is not known if the subject is in the reference database.[55]

3.1. Automated fingerprint identification

An automated fingerprint identification system (AFIS) works by extracting mathematical representations (templates) from fingerprint images (sample) to facilitate the comparison of fingerprints. There are two main fingerprint matching techniques: minutiae matching (comparing the location and direction of minutiae points) and pattern matching (comparing two images to see how similar they are).[56] It is also possible to 'lift' fingerprints from a surface touched by an individual (latent fingerprints) and digitalise them, though these generally present low-quality features.

Depending on the number of fingerprints used and on the origin of fingerprints, there are different identification scenarios (use cases). A typical use case involves comparing the fingerprints (ten print) of a person subject to a police or border check against a central database containing sets of fingerprints (ten print database) is illustrated below.

Figure 2: The steps in the fingerprint identification process (print vs ten print scenario)



Source: Beslay and Galbally, 2015, p. 34.

3.1.1. Fingerprint identification in the EU information systems

Automated fingerprint identification is currently used in the SIS, Eurodac and the VIS, and will also be implemented in the EES and the ECRIS-TCN.

[55] FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, November 2019, p. 7.

[56] R. King, 'Explainer: Fingerprint Matching', biometricupdate.com, December 2015.

From the very inception of the **Schengen Information System**, it has been possible to store fingerprints and photographs in it. These can be used to verify a person's identity following a successful search based on alphanumeric data. The use of fingerprint searches to identify a person only became possible after the implementation of the AFIS in the SIS in 2018[57] (following a positive report[58] on the readiness of the technology). According to the new legal bases of the SIS, the use of the AFIS is mandatory for all Schengen countries: they must carry out fingerprint searches in cases where the identity of the person cannot be ascertained by other means. According to a 2019 report by the Commission's Joint Research Centre (JRC), in 2018, only around 0.005 % of SIS searches were processed by the AFIS.[59] In its 2020 report on the implementation of the updated legal bases of the SIS, the Commission found that, by September 2019, only 19 Member States had deployed the AFIS search functionality.[60] As reported by eu-LISA, 3.7 billion total searches were carried out in the SIS in 2020.[61] Seventeen EU/Schengen countries carried out biometric searches in the system. With regard to funding to support Member States in their efforts to upgrade their national systems, a first amount of €18.4 million was committed in 2019 (the total additional budget is €36.8 million).

Fingerprint searches (using ten prints sets) were implemented in **Eurodac** as from its rollout in 2003. Since July 2015, law enforcement personnel have also been allowed, under certain conditions, to query the system using latent fingerprints. In 2020, the Member States transmitted about 645 000 sets of fingerprints to Eurodac, which included 208 searches carried out by law enforcement personnel from the Member States and Europol (using non-latent and latent fingerprints).[62]

Visa applicants' fingerprints are introduced into the **Visa Information System** during the application procedure and are verified against the database for possible duplicates/matches. Fingerprint searches in the VIS are carried out at the EU external borders for verification and, if necessary, identification (verification in the VIS became mandatory in October 2014). As reported by eu-LISA,[63] the VIS contained 41 million fingerprint sets in September 2017; 30 million more sets (applications with fingerprints) were registered by September 2019. Seventeen million biometric (using fingerprints) authentications and 7 million biometric searches were conducted in the VIS throughout 2019. Under certain conditions, law enforcement officers can also conduct searches in the VIS, but not with latent fingerprints. Between September 2017 and September 2019, they carried out almost 19 000 searches in the VIS. The current proposal to revise the VIS provides for the possibility to search the system using latent fingerprints where there are reasonable grounds to believe that a perpetrator or a victim may be registered in the VIS.

The Entry/Exit System will store fingerprints of visa-exempt third-country nationals for the purpose of verification and identification and will allow searches with latent fingerprints.

---

57 eu-LISA, eu-LISA successfully launches SIS II AFIS Phase One, 6 March 2018.

58 L. Beslay and J. Galbally, Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II), JRC report, 2015.

59 J. Galbally, P. Ferrara, R. Haraksim, A. Psyllos, and L. Beslay, Study on Face Identification Technology for its Implementation in the Schengen Information System, JRC report, 2019, p. 19.

60 European Commission, Report on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS), February 2020.

61 eu-LISA, SIS II – 2020 Statistics, March 2021.

62 eu-LISA, Eurodac – 2020 Statistics, March 2021.

63 eu-LISA, Report on the technical functioning of the Visa Information System (VIS), August 2020.

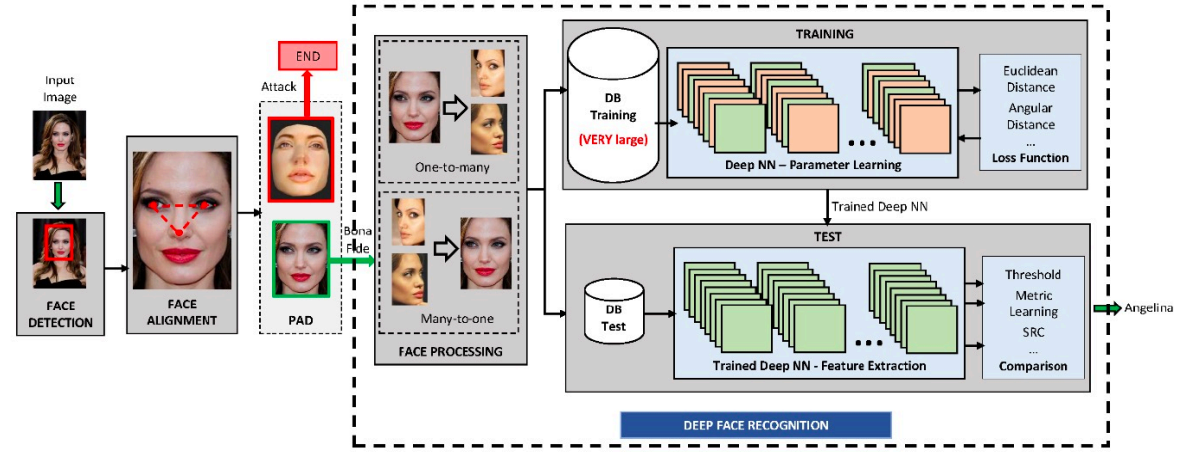
The European Criminal Record Information System for third-country nationals will make it possible to process fingerprint data of third-country nationals so as to check whether any of the Member States hold criminal record information about them.

3.2. Face recognition

The development of AI thanks to deep learning has led to significant advances in computer vision.[64] Deep learning AI is a subset of machine learning AI that relies on artificial neural networks (NN) to identify patterns in a dataset. Deep learning algorithms can be applied to supervised learning tasks (where data are human-labelled in advance) and unsupervised learning tasks (where no data labelling is necessary).

A deep learning-based face recognition system typically detects a face, normalises the image (localises face landmarks), and extracts facial features in order to compare them against one or many reference faces[65] (see Figure 3).

Figure 3: how a deep learning-based face recognition system works



Source: Galbally et al., 2019, p. 33.

Automated border control (ABC) at airports is the most common example of how face recognition technology is used. An ABC system is 'an automated system which authenticates the electronic machine-readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records, then determines eligibility of border crossing according to the pre-defined rules'.[66] Today's ABC systems support a number of biometrics, including facial recognition and (less often) iris recognition. Face recognition-based ABC works by comparing the live captured facial image of the traveller against the facial image stored on the chip of his or her travel document. This makes it possible to verify a traveller's identity (along with other checks), without the need to store the new facial images in a database.

With the gradual adoption of biometric passports across the world, ABC gates using face recognition technology are becoming a common feature of airport security checks. While the US[67] has been at

64 DeepAI, 'What is Computer Vision?'.

65 Galbally et al., Study on Face Identification, 2019.

66 Frontex, Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, September 2015, p. 10.

67 A. Al-Heeti, 'US border protection used facial recognition on 23 million travelers in 2020. That's up by 4 million from 2019', cnet.com, 11 February 2021.

the forefront of this development, a recent report[68] also provides examples of face recognition-based ABC gates at EU airports (in Italy and Portugal).

Face recognition technology can also be used for real-time surveillance of airports and other public spaces by analysing live stream video from CCTV cameras. This works by extracting facial images captured by cameras and comparing these against facial images of persons included in watch lists. As uncovered by a 2020 report,[69] face recognition systems are rapidly deployed in Europe for public surveillance, not only at airports but also in schools, stadiums and event venues.

In 2017, Belgium tested a face recognition system at Brussels Airport for live identification of people of interest (from a watch list). The system was put on hold following the intervention of the Supervisory Body for Police Information, which discovered that the cameras continued to be active after the test (though were not linked to a watch list).[70]

3.2.1. Face recognition in EU information systems and exchange

Face recognition technology is currently not used in any EU centralised information systems. However, in the near future all these systems except ETIAS are expected to process facial images for the purpose of verification or identification.

About 30 % of alerts in the **Schengen Information System** contain facial images[71] (there were about 965 000 alerts on persons in the SIS in 2020[72]). The legal bases of the SIS allow for the implementation of face recognition functionality in the system, provided that the technology has reached a sufficient level of readiness and availability. To this effect, a JRC study in 2019[73] concluded that automatic face recognition technology could be integrated in the SIS.

The outstanding proposal for revising **Eurodac** envisages the introduction of facial images to enable searches with facial images in the system. According to the proposal, eu-LISA will be tasked to carry out a study on the technical feasibility of implementing face recognition technology in Eurodac.

The Visa Information System stores digital photos of visa applicants (the system stored about 68 million photos in 2019[74]). The current proposal to revise the VIS provides for the collection of live facial images to enable biometric matching using face recognition technology.

The Entry/Exit System will process facial images for the purpose of verifying and, under certain conditions, establishing a person's identity. Within a period of two years following the start of operations of the EES, the Commission should produce a report on the quality standards of facial images stored in the VIS in view of using these images for the verification of the identity of third-country nationals subject to a visa requirement (without further storing these facial images in the EES). As reported by eu-LISA,[75] the new system will rely on machine learning techniques for

---

68 F. Chiusi, Fabio, S. Fischer, N. Kayser-Bril and M. Spielkamp (eds), 'Automating Society Report 2020', AlgorithmWatch, October 2020.

69 ibid.

70 B. Peeters, 'Facial recognition at Brussels Airport: face down in the mud', KU Leuven, 17 March 2020.

71 Galbally et al., Study on Face Identification, 2019, p. 19.

72 eu-LISA, SIS II – 2020 statistics, March 2021.

73 Galbally et al., Study on Face Identification, 2019.

74 eu-LISA, Report on the technical functioning of the Visa, 2020, p. 10.

75 eu-LISA, Artificial Intelligence in the Operational Management, 2020.

biometric matching. In 2019, the Commission adopted specifications[76] for the quality, resolution and use of fingerprints and facial images for biometric verification and identification in the EES.

The European Criminal Record Information System for third-country nationals will allow using facial images (solely) to confirm the identity of a third-country national who has been identified as a result of an alphanumeric search or a search using fingerprint data. The Commission could, after assessing the availability and readiness of the technology, adopt delegated acts concerning the use of facial images for the purpose of identifying third-country nationals in order to ascertain whether any Member States hold information on previous convictions.

In line with the interoperability framework, the Common Identity Repository will become a new shared component of the EES, the VIS, ETIAS, Eurodac or ECRIS-TCN, storing all the identity data, travel document data and biometric data of persons registered in these systems. The shared Biometric Matching Service will store the templates of all biometric samples from the SIS, Eurodac, the VIS, and the EES.

Outside the centralised systems, EU Member States exchange information through a number of police cooperation frameworks. **The Prüm framework** (defined by Council Decisions 2008/615/JHA and 2008/616/JHA) allows a Member State to query DNA, dactyloscopic and vehicle registration data in one or several other Member States' national databases. In case of a 'hit', the authorities in a Member State can request case-related data from the Member State holding the information.

In 2020, the Commission published a roadmap[77] for the review of the Prüm framework, suggesting a number of possible improvements, including the possibility to exchange facial images, develop central components for searching and comparing data, and add new functionalities (such as using DNA and fingerprint queries for searching missing persons and unidentified human remains). A 2020 study[78] on possible improvements of the Prüm framework recommended the adoption of the exchange of facial images, after considering 'the maturity of the technology and its capability within the context of forensic law enforcement'. Another study on the use of facial recognition for the investigation of crime across EU Member States is forthcoming in the context of the EU-funded project, Towards the European Level Exchange of Facial Images.[79]

Table 1 – Overview of data processed in EU information systems for borders and security

Information regarding	Data	SIS	Eurodac	ECRIS-TCN	VIS	EES	ETIAS
Identity	DNA sample	Yes					*
	Palmprint	Yes					
	Photograph	Yes			Yes		**
	Fingerprint	Yes	Yes	Yes	Yes	Yes	
	Facial image	Yes	*Proposed*	Yes	*Proposed*	Yes	
	Name(s)	Yes	*Proposed*	Yes	Yes	Yes	Yes
	Gender/sex	Yes	Yes	Yes	Yes	Yes	Yes
	Nationality(ies)	Yes	*Proposed*	Yes	Yes	Yes	Yes
	Date of birth	Yes	*Proposed*	Yes	Yes	Yes	Yes
	Travel document info		*Proposed*	Yes	Yes	Yes	Yes
	Place/country of birth	Yes	*Proposed*	Yes	Yes		Yes

[76] European Commission, Implementing decision laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the EES, 25 February 2019.

[77] European Commission, Strengthening the automated data exchange under the Prüm framework, Combined evaluation roadmap / inception impact assessment, 2020.

[78] Deloitte, 'Study on the feasibility of improving information exchange under the Prüm decisions', May 2020.

[79] Towards the European Level Exchange of Facial Images, https://www.telefi-project.eu/.

	Current occupation						Yes
	Current address						Yes
Security	Security risk	Yes	*Proposed*				
	Reasons for alert	Yes					
	Action to be taken	Yes					
Entry /exit	Date and place of entry/exit					Yes	
	Decision on refusal of entry	Yes					
	Place/date of apprehension		Yes				
	Place/date of disembarkation		*Proposed*				
	Overstaying flag					Yes	
	Return decision	Yes	*Proposed*				
Asylum	Place/date of application		Yes				
	MS of origin		Yes				
	MS responsible for application		*Proposed*				
	Asylum processing date		Yes				
	MS holding the criminal record			Yes			
Visa	Info on visas (visa history)		*Proposed*		Yes	Yes	
	Visa application info				Yes		
	Links to other visa applications				Yes		
	Results of VIS verifications				*Proposed*		
Travel	Purpose of travel				Yes		
	Intended route (entry, exit)				Yes		
	Intended residence/ address				Yes		Yes
About other persons	Parents' names			Yes			Yes
	Visa sponsor (name, address)				Yes		
	Persons filling the application						Yes
	EU family member						Yes
Declaration	Declared convictions						Yes
	Stays in war/conflict zones						Yes
	Declared expulsions						Yes
Other	IP address (application)						Yes

** Light blue area = biometric data; ** dashed line area = data included in the Common Identity Repository*

Data source: author's compilation from publicly available sources.

4. Emotion detection AI

Emotion detection technologies aim to detect mental states and emotions based on the examination of facial expressions, often in conjunction with other physiognomic characteristics (such as gaze direction, gesture, voice, heart rate, body temperature, skin conductivity, etc.).[80]

AI-based emotion detection systems largely rely on the theories developed by American psychologist, Paul Ekman, who believes that lying triggers non-verbal behavioural traces that could be recognised by analysing facial expressions. Building on Ekman's claim that human emotions can be classified in six universal basic categories (anger, disgust, fear, happiness, sadness and surprise), AI researchers have sought to automate the recognition of these basic emotions as they appear in facial expressions (though Ekman has reportedly expressed doubt about the reliability of automated detection technologies).[81]

AI-based emotion detection applications are already deployed in a number of areas and contexts, where they are used to monitor mental health, detect fraudulent insurance claims, monitor

[80] Sánchez-Monedero and Dencik, 'The politics of deceptive borders', 2020.

[81] K. Crawford, *The Atlas of AI*, Yale University Press, 2021.

students' engagement (including to help children with autism develop social and emotional skills), assess job candidates, and detect potential shoplifters. Such applications are also advertised for law enforcement purposes, such as crime prevention, security checks and border control.

In 2016, researchers at Shanghai Jiao Tong University claimed they had developed a facial expression analysis algorithm that could distinguish between portraits of criminal convicts and non-criminals.[82] In 2017, two researchers at Stanford University claimed to have invented an AI 'gaydar' that could identify gay men from analysing pictures (with 81 % accuracy).[83] The researchers were also reported[84] to have claimed that their algorithms could be trained to measure a person's intelligence and criminal inclinations. More recently, in 2020, researchers at Harrisburg University announced[85] they had developed a face analysis software that could predict if someone was a criminal. In the meantime, a great deal of companies have started applying these novelties in practice. For example, an Israeli company claims to be able to 'detect, focus and apprehend potential terrorists or criminals before they have the opportunity to do harm'.[86]

In the context of borders, in 2007, the US Transportation Security Administration rolled out the Screening of Passengers by Observation Techniques system to detect air travellers' expressions of fear and stress that could lead to identifying potential terrorists. The system was criticised as both ineffective and discriminatory.[87] In 2021, the UK Border Agency tested a tool to evaluate stress, anxiety and deception at the immigration desk, based on a facial and thermal analysis.[88]

4.1. Emotion detection AI at EU borders

While there are no AI-based emotion detection systems implemented at the EU borders at the moment, a number of EU-funded research projects have sought to develop AI systems aiming to capture human emotions and to detect deception in the context of border control.

The project, Intelligent Portable Control System (iBorderCtrl),[89] which ran between 2013 and 2019 and received €4.5 million in EU funding, aimed to develop a decision support system for border checks that included an automated deception detection tool. Under the project, pilot tests were carried out at several land border crossing points in Hungary, Greece and Latvia. The deception detection tool envisaged subjecting a traveller to an interview with an avatar in order to identify 'biomarkers of deceit', non-verbal facial micro-expressions that are associated with lying (such as left eye blink, increase in face redness, head movement directions).[90] The researchers reported an accuracy rate of 73-75 % for detecting deception and truthfulness. The accuracy of the results and the general approach and implications of the project have been strongly contested (see Section 7.1.1).

---

82 X. Wu, Xiaolin, and X. Zhang, 'Automated inference on criminality using face images', arXiv (preprint), 2016.

83 M. Kosinski and Y. Wang, 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images', *Journal of Personality and Social Psychology*, 114 (2), 2018.

84 S. Levin, 'Face-reading AI will be able to detect your politics and IQ, professor says', *The Guardian*, 12 September 2017.

85 S. Fussell, 'An Algorithm That 'Predicts' Criminality Based on a Face Sparks a Furor', *Wired*, 24 June 2020.

86 https://www.faception.com/

87 O. Schwartz, 'Don't look now: why you should be worried about machines reading your emotions', *The Guardian*, 6 March 2019.

88 Sánchez-Monedero and Dencik, 'The politics of deceptive borders', *Information, Communication and Society*, 3 August, 2020.

89 European Commission, Intelligent Portable Border Control System, Community Research and Development Information Service (CORDIS).

90 Sánchez-Monedero and Dencik, 'The politics of deceptive borders', 2020.

Frontex collaborated with the US National Center for Border Security and Immigration (BORDERS) in the context of the research project on Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR).[91] AVATAR developed a deception-detection system based on the analysis of facial expressions, voice, body and eye signals. The collaboration between Frontex and BORDERS took place through a number of annual workshops, experiments and field tests. An AVATAR field test was carried out in 2013 at the Henri Coandă International Airport of Romania.[92]

5. Algorithmic profiling

Risk assessment algorithms and decision support systems in immigration and border management are increasingly rolled out globally.[93] AI algorithms can also be used to sift through data (personal and non-personal) in order to identify unknown persons who may be of interest to the authorities.

At the EU borders, automated risk assessments are carried out in the framework of information exchange on passengers and in the context of the VIS (and the future ETIAS). Risk assessments and analyses may rely on aggregate data extrapolated from all information systems. For example, the updated SIS regulation (on borders) tasks eu-LISA to provide Frontex with 'additional specific statistics… to be used for the purpose of carrying out risk analyses and vulnerability assessments' (Article 40).

5.1. Advance passenger information and passenger name records

Council Directive 2004/82/EC on advanced passenger information (the API Directive) obliges air carriers to transmit, upon request, passenger data (biographic information and travel route information) to the Member State of destination prior to the flight's take-off, for inbound flights from a third country. The primary objective of advance passenger information (API) is enforcing border control and preventing irregular migration. The directive also allows using API data for law enforcement purposes if authorised by national law. The aim is to detect unknown persons of interest before they come to the border.

A 2020 evaluation study[94] of the API Directive found that only 13 Member States had established targeting centres for processing API data to enable them to conduct automated risk assessment of travellers based on collected travel intelligence and tactical risk analysis. Some Member States collect a number of additional API data (beyond the required minimum), such as data for other modes of transport (sea carriers by 10 Member States; trains by four Member States; and coaches/buses by one Member State). In the context of a planned review of the API Directive, the Commission envisages the possibility of making the collection of API data mandatory for other modes of transport as well.[95]

Directive (EU) 2016/681 on passenger name records (the PNR Directive)[96] obliges the Member States to collect and exchange passenger data (travel dates, itinerary, ticket information, contact details, means of payment, and baggage information) from airline companies operating extra-EU flights for

91 University of Arizona, Automated Virtual Agent for Truth Assessments in Real-Time.

92 Frontex, Appraising the AVATAR for Automated Border Control Results of a European Union Field Test of the AVATAR System for Interviewing and Passport Control, October 2014.

93 Molnar and Gill, 'Bots at the Gate', 2018, p. 3.

94 ICF and Unisys, 'Study on Advance Passenger Information (API). Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data', February 2020.

95 European Commission, Advance Passenger Information – API, Roadmap and Inception impact assessment, 2020.

96 European Commission, Passenger Name Record (PNR), Migration and Home Affairs.

the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Under certain conditions, the Member States may transfer PNR data to third countries on a case-by-case basis. The EU has concluded international PNR agreements with Australia and the USA; PNR-related negotiations with Japan started in 2020. A PNR agreement with Canada was suspended by the European Court of Justice (ECJ) due to inadequate fundamental rights safeguards.

PNR can be used to identify unknown persons who might be of interest, such as 'passengers whose travel behaviours are atypical or fit the travel patterns usually encountered in the case of offenders'. This is done, in practice, 'by comparing PNR data, through automated means, against combinations of predetermined fact-based risk indicators'.[97] These indicators are set by the national passenger information units and are updated on the basis of new data and patterns available in the system. Europol provides assistance to the Member States in the development of pre-determined criteria through its Travel Intelligence Task Force. The PNR Directive allows for automated processing of PNR data but maintains that any positive match resulting from the automated processing of such should be individually reviewed by non-automated means.

In its 2020 review report[98] of the PNR Directive, the Commission found that 24 out of 26 Member States had transposed the directive and that further assessment was needed both from the point of view of its practical implementation and of a possible extension of its scope. In its roadmap[99] to update the EU approach to PNR transfers, the Commission suggested several options, including adopting a regulation setting out the conditions and criteria for transmitting the data and switching to a multilateral PNR agreement.

5.2. ETIAS screening rules

In the context of ETIAS, visa-exempt third-country nationals will be assessed against risks of irregular migration, security or public health. Applications will be automatically checked against all other relevant EU information systems, Europol data, and Interpol databases. The applicants' personal data will also be automatically checked against the new ETIAS watchlist and against specific risk indicators. Specific screening rules will be built into an algorithm that will make it possible to identify travellers that fit pre-defined risk profiles. Risk indicators will consist of a combination of data including age range, sex, nationality, country and city of residence, level of education (primary, secondary, higher or none), and current occupation (job group). In the case of a 'hit', the application will be referred to an officer for review.

eu-LISA suggested that 'an additional level of automation or analytics based on AI or machine learning could be introduced when dealing with any "suspicious" applications'.[100] A 2020 study for the Commission also envisaged an AI tool in ETIAS for 'individual risk assessment in case of a 'hit' in the first automatic risk assessment, facilitating further review by a member state'.[101]

---

97 European Commission, Staff working document accompanying the report on the review of Directive 2016/681 on the use of passenger name record (PNR) data, July 2020, p. 24.

98 European Commission, Report on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, July 2020.

99 European Commission, Roadmap on the external dimension of the EU policy on Passenger Name Records, 2020.

100 eu-LISA, Artificial Intelligence in the Operational Management, 2020, p. 30

101 Deloitte, 'Opportunities and challenges', 2020, p. 19 and pp. 91-92.

5.3. Proposed risk indicators in the VIS

Regulation (EC) No 810/2009 (the Visa Code) provides for an individual assessment of risks of illegal immigration or security and lists a number of factors to be considered when assessing these risks (including socioeconomic structure of the host country, local information on social security, illegal immigration routes, and information on refusals).

The current proposal on the revision of the VIS Regulation introduces new specific risk indicators containing data analytics rules, statistics generated by other information systems (abnormal rates of refusals of visa applications due to an irregular migration, security or public health risk – sourced from the VIS; abnormal rates of overstayers and refusals of entry for a specific group of travellers holding a visa – sourced from the EES), and data from the Member States (abnormal rates of overstayers and refusals of entry) and the European Centre for Disease Prevention and Control (ECDC) (epidemiological surveillance information). The proposal lists the categories of data to be included in the definition of indicators and provides for a number of fundamental rights safeguards (prohibition of the use of indicators based solely on a person's sex or age or on sensitive personal data).

A 2019 study[102] on visa digitalisation envisaged establishing 'a unique digital visa portal [that] will standardise the visa practices across Schengen countries' consulates based on data-driven algorithms that translate the common visa policy into checks and alerts'. The interactive data-driven algorithms of the online application will also 'enable the behaviour of travellers to be checked, hence activating a behind-the-scenes risk analysis'. A 2020 study for the Commission envisioned the creation of an AI triaging tool 'to classify visa applicants based on an initial assessment'. The study also proposed a tool for the 'identification of irregular travelling patterns as an additional piece of risk analysis' using data from different sources such as the VIS, the EES and PNR.[103]

6. AI tools for migration monitoring, analysis and forecasting

AI-assisted analytics of migration flows and cross-border crime trends (threat detection and risk analysis) are becoming a common tool for border control.[104] At EU borders, several EU agencies use AI tools and services to monitor, analyse and forecast migration trends and security threats.

A 2020 study[105] for the Commission analysed the feasibility of developing a forecasting and early warning AI tool to assess the direction and intensity of irregular migratory flows to and within the EU and to provide early warnings and forecasts. The study concluded that 'a well-performing forecasting system can be built', though its reliability could not be properly assessed in advance.

6.1. Frontex risk analysis

Frontex plays a key role in monitoring migratory flows and in carrying out risk analysis as regards all aspects of the integrated border management. The agency is responsible for EUROSUR, an integrated framework for the exchange of information at EU external borders.

---

[102] Deloitte, 'Study on the feasibility and implications of options to digitalise visa processing', September 2019.

[103] Deloitte, 'Opportunities and challenges', 2020, p. 16 and pp. 89-90.

[104] Frontex, Artificial Intelligence-based capabilities, final report, 17 March 2021.

[105] Ecorys, Feasibility study on a forecasting, 2020.

According to a 2019 Commission answer[106] to a parliamentary question, 'Frontex does not use AI technology for the time being to prepare the European Situational Picture or the Eurosur Fusion Services'. However, in September 2019 Frontex published a tender[107] for a social media analysis service concerning irregular migration trends and forecasts to support the planning and the evaluation of joint operations coordinated by Frontex. The prospective monitoring service included a 'sentiment analysis' component to assess 'what people, on the internet and social media, are saying and feeling and where they're saying it, with relevance to irregular migration'. The call was cancelled after the entry into force of the new Frontex Regulation.

The 2021 Commission implementing regulation on the situational pictures of EUROSUR[108] provides that Member States and Frontex 'should develop technical interfaces to foster machine to machine interconnections and use decision support tools to assist EUROSUR operators in their tasks'.

As part of its mandate, Frontex monitors and contribute to developments in research and innovation relevant to the management of external borders. It follows up and provides assistance to the Commission on programming, monitoring and the uptake of projects in the area of border security (Horizon programme),[109] and participates in pilot projects testing border technologies.

The 2021 Frontex study[110] on AI technologies and capabilities for border security identified a number of promising technology areas, including automated border control (e-gates, document scanning and verification, facial recognition and other biometric verification), maritime domain awareness, surveillance towers and small autonomous unmanned aerial systems.

6.2. EASO monitoring tools

The European Asylum Support Office (EASO) fosters EU Member States' cooperation on asylum. EASO developed an Early Warning and Forecasting System to monitor the situation in third countries and to forecast the number of asylum applications that EU Member States can expect. According to a 2020 EASO report,[111] the agency 'uses machine learning to analyse big data on conflict and disruptive events in countries of origin and transit in order to clarify the root causes of individual displacement events'. The aim is 'to understand and predict arrivals of third-country nationals that might exert particular pressure on national asylum and reception authorities'.

Until 2019, EASO produced social media monitoring reports based on analysing posts of Facebook, Instagram, YouTube, and Twitter users that were related to EU asylum and migration issues (within the Arabic, Pashto, Dari, Urdu, Turkish, Russian, Tigrinya, Kurmanji Kurdish, Pidgin English, Hausa, Edo, as well as French communities).[112] In 2019, the European Data Protection Supervisor (EDPS) issued a temporary ban on the production of social media monitoring reports due to issues of legality and data protection concerns.[113]

---

106 Parliamentary question, Answer given by Ms Gabriel on behalf of the European Commission, 28 March 2019.

107 eTendering, Frontex/OP/534/2019/DT, 2019.

108 European Commission, Implementing regulation on the situational pictures of the European Border Surveillance System (EUROSUR), 9 April 2021.

109 Frontex, EU research.

110 Frontex, 'Artificial Intelligence - based capabilities', 2021.

111 EASO, EASO Asylum Report, 2020, p. 57.

112 EASO, Record of data processing activity for EASO's Social Media Monitoring Reports, 2019.

113 EDPS, Letter concerning a consultation on EASO's social media monitoring reports, 14 November 2019.

6.3. Europol innovation hub

The European Union Agency for Law Enforcement Cooperation (Europol) supports Member States' actions and their cooperation in preventing and combating serious crime affecting two or more Member States. In 2019, Frontex and Europol established a Future Group[114] on travel intelligence and border management to discuss operational issues related to the implementation of EU smart borders, interoperability and PNR.

In October 2019, ministers at the Justice and Home Affairs (JHA) Council agreed to establish an innovation hub at Europol to act as an observatory of new technological developments and drive innovation in the field of internal security. All JHA agencies were invited to participate in the hub. As part of the hub, a number of 'quick-win' projects were selected and are currently under preparation, including a project to develop accountability principles for AI used in the area of freedom, security and justice (Europol with the FRA, EASO and other EU agencies), and another project to develop AI initiatives in ETIAS (eu-LISA in cooperation with Frontex).[115]

In 2021, the Commission put forward a proposal[116] to revise Europol's mandate, whereby the agency would be allowed to process vast datasets, enabling it to 'play a key role in assisting Member States to develop new technological solutions based on artificial intelligence'.

Table 2 – Overview of key EU initiatives on the use of AI technologies at EU borders

EU actor(s) responsible	AI category	Type of initiative	Initiative (relevant objective)	Status
Commission / Council / EP	Biometric identification	Proposed legislation	Enabling face recognition in Eurodac	Proposed (2016)
Commission / Council / EP	Biometric identification	Proposed legislation	Enabling face recognition in VIS	Proposed (2018)
Commission / Council / EP	Algorithmic profiling	Proposed legislation	Enabling individual risk assessment in the VIS	Proposed (2018)
Commission / Council / EP	Migration monitoring	Proposed legislation	Revising Europol's mandate to boost data analytics and AI	Proposed (2020)
Commission / Council / EP	Biometric identification	Legislation	Enabling face recognition in the EES	Adopted (2017)
Commission / Council / EP	Biometric identification	Legislation	Enabling face recognition in the ETIAS	Adopted (2018)
Commission / Council / EP	Biometric identification	Legislation	Enabling face recognition in the ECRIS-TCN	Adopted (2019)
Commission / Council / EP	Algorithmic profiling	Legislation	Enabling individual risk assessment in the ETIAS	Adopted (2018)
Commission	Migration monitoring	Legislation	Foreseeing the use of decision support tools in EUROSUR	Adopted (2021)
Frontex	Migration monitoring	Tender	Establishing a Common Pre-frontier Intelligence Picture monitoring service	Cancelled (2019)
EASO	Migration monitoring	Policy	Providing an Early Warning and Forecasting System	Ongoing
EASO	Migration monitoring	Policy	Providing a social media monitoring service	Suspended (2019)
Europol	Algorithmic profiling	Policy	Support risk assessment and analysis in the framework of the PNR/API	Ongoing
Europol / EU agencies	Wide	Policy	Establishing a Europol innovation hub to support AI initiatives	Ongoing

[114] Europol, Future group on travel intelligence and border management – presentation, 18 December 2020.

[115] Council, EU Innovation Hub for Internal Security - state of play, 17 February 2021.

[116] European Commission, Proposal for a Regulation amending Regulation (EU) 2016/794, 9 December 2020.

Commission	Biometric identification	Research Project	Mapping the use of face recognition for the investigation of cross-border crime	Ongoing
Commission	Emotion detection AI	Research Project	iBorderCtrl: developing a deception detection tool for border checks	Finalised (2019)
Commission	Wide	Study	Mapping opportunities and challenges for the use of AI in border control, migration and security	Delivered (2020)
Commission	Wide	Study	Exploring the possibilities for the development of data spaces in law enforcement	Delivered (2021)
Commission	Biometric identification	Study	Assessing the feasibility of using face recognition in the SIS	Delivered (2019)
Commission	Biometric identification	Study	Assessing the feasibility of using face recognition in the Prüm framework	Delivered (2020)
Commission	Algorithmic profiling	Study	Supporting visa digitalisation ('behind the scenes' data analytics)	Delivered (2020)
Commission	Migration monitoring	Study	Assessing the feasibility of establishing an AI-based forecasting and early warning tool for migration	Delivered (2020)
Frontex	Wide	Study	Mapping AI technologies and capabilities for border security	Delivered (2021)
Eu-LISA	Wide	Study	Devising the agency's approach to AI	Delivered (2020)

Data source: author's compilation from publicly available sources.

7. Key issues

7.1. Reliability of technologies

7.1.1. Accuracy of biometric identification

Automated fingerprint identification technologies have been around for a while and have been used successfully in Eurodac since its establishment. The 2015 report[117] on the readiness of the AFIS in the SIS found that the technology has a high accuracy, with error rates of around 0.1 %. The study listed 19 recommendations for the roll-out of the technology, including different measures to ensure the highest possible quality of the stored data.

The accuracy of the AFIS may depend on the subjects' physical characteristics, age being of particular relevance in this regard, because fingerprint characteristics change until adolescence and during old age. In 2013 and 2018, the JRC carried out two studies[118] on the feasibility of using children's fingerprints. The studies concluded that the fingerprint recognition of 6-12 year-old children is achievable with a satisfactory level of accuracy under certain conditions (including appropriate training of operators). Another study[119] for the Commission, published in 2018, found that lowering the fingerprinting age from 12 to 6 in the context of the VIS would be feasible and could bring additional benefits by strengthening the prevention of and fight against children's rights abuses.

[117] Beslay and Galbally, 'Fingerprint identification technology', 2015.

[118] G. Schumacher, Fingerprint Recognition for Children, JRC technical report, 2013; L. Beslay, J. Galbally and R. Haraksim, Automatic fingerprint recognition: from children to elderly. Ageing and age effects, JRC technical report, 2018.

[119] Ecorys, BV Fraunhofer IGD, and Vrije Universiteit Amsterdam, 'Feasibility and implications of lowering the fingerprinting age for children and on storing a scanned copy of the visa applicant's travel document in the Visa Information System (VIS)', March 2018.

The quality of fingerprint images can be affected by a number of other factors, such as the subject's occupation, motivation/collaboration, temporary or permanent cuts, as well as environmental circumstances (e.g. dryness/wetness conditions, temperature), dirt, residual prints on the sensor surface, etc.[120] Moreover, new technological developments, such as the introduction of new scanning technologies, require constant evaluation and testing.[121]

Face recognition technology has made significant progress in recent years.[122] Despite this, however, it 'remains far more prone to errors than other biometrics'.[123] There are plenty of examples of unsuccessful attempts to use face recognition technologies. For instance, a face recognition system installed at Belgium's Brussels Airport (e-gates) was scrapped in 2020 due to persistent errors and inefficiency (the e-gates required more staff than a conventional check).[124]

The accuracy of face recognition technologies is highly dependent on the quality of the images, including images captured during the collection of biometrics (biometric enrolment) and images used to train AI algorithms (training dataset). During enrolment, poor quality images taken at e-gates or through a CCTV camera under variable environmental conditions may result in less accurate results. As in the case of automated fingerprint identification, changes in a person's physical characteristics over time may also affect the accuracy of FRT. For example, changes in the facial shape of a child also have an impact on the reliability of a match.[125] Recent research has a found 'a considerable degradation in performance' for face recognition algorithms on children as compared to the performance obtained on adults.[126]

The 2019 JRC study on the introduction of face identification technology (ABIS-Face) in the SIS recommended to always use a live picture of the traveller and to avoid using the face image stored in the passport chip because its low resolution decreases accuracy. However, the EES regulation allows operators using the EES to exceptionally extract facial images from the chip of the electronic machine-readable travel document, provided that the image has 'sufficient image resolution and quality to be used in automated biometric matching'. The JRC study on the SIS also recommended to store 'additional off-angle (yaw) images' for 'future potential uses of the ABIS-Face, like for example consultation using images acquired in unconstrained environments (e.g. coming from

Measures of accuracy of face recognition systems

The accuracy of face recognition systems is measured in terms of a trade-off between false acceptance and false rejection.

False acceptance (measured as false positive identification rate or the false match) occurs when a system accepts a facial recognition claim that should have been rejected. False rejection (measured as the false non-match rate, or the false negative identification rate), occurs when the system rejects a facial recognition claim that should have been accepted.

The confidence threshold is a benchmark score that determines the acceptable level of estimated similarity before a recognition (match) will occur.

Source: Israel, 'Facial recognition at a crossroads' 2020.

120 Beslay and Galbally, 'Fingerprint identification technology', 2015, p. 29.

121 See, for example, a report on the use of multispectral imaging scanning technologies in Eurodac: eu-LISA, Eurodac: MSI/Optical Scan Test Study Summary Report, 2020.

122 NIST, Ongoing Face Recognition Vendor Test report, Part 1: Verification, 2019; NIST, Face Recognition Vendor Test report, Part 2: Identification, 2019.

123 Israel, 'Facial recognition at a crossroads', 2020, p. iv.

124 *The Bulletin*, '"A fiasco": Brussels Airport scraps e-passport gates', 16 February 2020.

125 FRA, Under watchful eyes: biometrics, EU IT systems and fundamental rights, 2018.

126 N. Srinivas, K. Ricanek, D. Michalski, D. S. Bolme and M. King, 'Face recognition algorithm bias: Performance differences on images of children and adults', Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019.

video surveillance footage)'.[127] However, the quality of images extracted from video footage may be insufficient to produce accurate matches using face recognition technology.

A 2018 FRA study identified data quality issues in all existing EU information systems. For example, the study found cases in the VIS where biometrics were attached to the wrong application file, resulting in false matches.[128] Data quality issues in EU information systems (more particularly, in the VIS), were also highlighted by a 2019 special report by the European Court of Auditors (ECA).[129]

Face recognition algorithms deliver probabilities of matches, and thus acceptable error rates need to be defined in advance. For example, the Commission's specifications on the use of biometrics in the EES[130] established, for identification based on facial images, a maximum false positive identification rate (the proportion of returned matches during a biometric search that do not belong to the checked traveller) of 0.1 % (1 per 1 000), and a false negative identification rate (the proportion of missed matches) of 1 %. When dealing with a massive number of applications, a false positive identification rate of 0.1 % may result in a great number of people being negatively affected (e. g. every 1 000 people in 1 000 000 searches).

7.1.2. Accuracy of emotion detection AI

There are serious concerns about the scientific basis of AI systems aiming to detect emotions from facial expressions. A 2019 review[131] of the literature found that facial expressions and perceptions thereof vary considerably across cultures and situations, and even within a single person. The authors identified three key shortcomings of these technologies: limited reliability (emotion categories are neither reliably expressed through, nor unequivocally associated with, a common set of facial movements); lack of specificity (facial expressions do not perfectly match emotion categories); and limited generalisability (the effects of context and culture are not sufficiently considered). Reliability issues may also arise when deploying the system in real-life situations, for example, when dealing with subjects who actively seek (and train themselves) to fool the system.[132]

In the case of the US Screening of Passengers by Observation Techniques system, a 2013 review[133] by the US Government Accountability Office found limited scientific evidence 'that behavioural indicators can be used to identify passengers who may pose a threat to aviation security' and questioned the effectiveness of the programme. Moreover, a study by the American Civil Liberties Union (ACLU) concluded that the programme resulted in racial profiling.[134]

The EU project iBorderCtrl has triggered significant criticism concerning its scientific validity, reliability and social impact. With respect to reliability, a 2020 paper[135] found limitations regarding the applicability of the model in a real-life context and concluded that it 'is very unlikely that the tool

---

127 Galbally et al., 'Study on Face Identification', 2019, p. 16.

128 FRA, Under watchful eyes, 2018, p. 16.

129 ECA, EU information systems supporting border control - a strong tool, but more focus needed on timely and complete data, 2019.

130 European Commission, Implementing decision laying down the specifications...', 2019.

131 L. F. Barrett, R. Adolphs, S. Marsella, A. M. Martinez, and S. D. Pollak, 'Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements', *Psychological science in the public interest*, 20(1), 2019.

132 S. Vargheze, 'The science behind the EU's creepy new border tech is totally flawed', *Wired*, 16 November 2018.

133 US Government Accountability Office, 'Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities', 13 November 2013.

134 ACLU,' Bad trip: Debunking the TSA's 'behavior detection' program', February 2017.

135 Sánchez-Monedero and Dencik, 'The politics of deceptive borders', 2020.

can work in practice'. A Greek civil society organisation obtained documents showing that no real traveller participated in the Greek pilot trials of the system.[136]

7.1.3. Accuracy of risk assessment algorithms

An additional challenge of data accuracy is posed by systems that rely on data supplied by external entities, such as airline companies (for the API and PNR), or self-declared information (e.g. from ETIAS applications). Such data may be more prone to errors than official records. Using data aggregated or mined from public sources (e.g. from social media accounts) also creates a high risk of introducing unreliable information into the risk profiling process. Profiling based on inaccurate data would compromise the effectiveness of police and border management work due to incorrect correlations and data distortions.[137]

Relying on information provided by third countries, either from the Interpol databases (e.g. for ETIAS checks) or under PNR agreements, also poses challenges. For example, some third countries' governments may use these channels to persecute political opponents.[138] In an answer[139] to a parliamentary question, the Commission acknowledged that the issue was 'of great concern'. In regard to the future connection of the Interpol databases with the European Search Portal and ETIAS, the Commission stated that 'Interpol will need to provide the necessary guarantees' and that, in any case, 'Member States will assess each request for travel authorisation individually, thus preventing that any potential abusive use of Interpol's databases translates into restrictions to travel to the EU'.

Unreliable technologies that result in inaccurate biometric matching may significantly affect a person's fundamental rights. This is particularly the case in the border and law enforcement contexts, where persons are usually in a weak position in relation to authorities and cannot easily contest a false biometric match or no match.

7.2. Fundamental rights

7.2.1. Bias and discrimination

There are benefits to be gained from a careful adoption of AI technologies, in terms of, for example, increased capacity to detect fraud and abuses, better and timely access to relevant information for taking decisions, and enhanced protection of vulnerable people. For example, the International Centre for Missing and Exploited Children announced in 2018 the launch of a global platform that uses image and video analysis tools to detect, analyse, and compare faces in imagery associated with open cases about missing children.[140]

In a 2019 analysis,[141] the FRA produced a long list of fundamental rights that may be affected when adopting face recognition technology, including human dignity, the right to respect for private life, the protection of personal data, non-discrimination, the rights of the child and the elderly, the rights

136 Homo Digitalis, 'Homo Digitalis' input to the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance', 13 May 2020.

137 FRA, Preventing unlawful profiling today and in the future: a guide, 2018, p. 119.

138 C. Jones, 'Automated suspicion: The EU's new travel surveillance initiatives', *Statewatch*, July 2020.

139 Parliamentary question, Answer given by Mr Avramopoulos on behalf of the European Commission, 5 April 2019.

140 International Centre for Missing and Exploited Children, 'International Centre For Missing & Exploited Children (ICMEC) Expands With AI, Biometrics, And Ad Tech', 27 November 2018.

141 FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, November 2019.

of people with disabilities, the freedom of assembly and association, the freedom of expression, the right to good administration, and the right to an effective remedy and to a fair trial.

Face recognition applications have been consistently shown to be less accurate for certain people such as women and people with darker skin tones.[142] A 2019 research report[143] by the US National Institute of Standards and Technology (NIST) tested 189 facial recognition algorithms and concluded that most of them exhibited bias. A 2020 survey of the literature on algorithmic bias in the context of biometrics found that 'demographic factors can have a large influence on various biometric algorithms and that current algorithms tend to exhibit some degree of bias with respect to certain demographic groups'.[144] Face recognition technology has sparked intense debates about its impact on fundamental rights, in particular when the technology applies to high-risk areas such as law enforcement.[145] For example, in January 2021 the Commission accepted a European Citizens' Initiative (ECI) put forward by the 'Reclaim Your Face' coalition, which calls for a ban on biometric mass surveillance.[146]

There are different causes of AI bias, including issues with the training datasets (skewed, incomplete, outdated or disproportionate data) and the algorithms (poorly designed, reflecting biased norms and prejudices, poorly implemented). According to an eu-LISA report, the challenge of training data can be addressed either by using representative data sets for training algorithms or by creating synthetic data sets with the characteristics that are representative of the population.[147] Whereas the former solution could pose data protection risks, the latter could lead to higher error rates associated with the use of synthetic data.

Developing and deploying AI algorithms requires making some 'technical' choices that can have important fundamental rights consequences. As a 2021 report for the Commission points out, 'violations of fundamental rights do not normally stem from the deployment of AI per se… rather, it is the intentional programming, and thus the conscious decision to programme and use AI systems by humans (alone or through organisations) that violate fundamental rights'.[148]

AI-based emotion detection technology is particularly problematic. This intrusive technology may have significant implications for certain people, in particular minorities and vulnerable people, including people who have tics or anxiety, or are neuroatypical. Given the potential of AI technologies for 'laundering' human prejudice, some blame these technologies for the recent resurgence of scientific racism.[149] Emotion detection AI research seems to be driven by a

---

142 J. Buolamwini, 'Algorithmic Bias: Automated Facial Analysis', MIT Media Lab, article published on www.poetofcode.com; A. Koene et al., A governance framework for algorithmic accountability and transparency, EPRS study, European Parliament, March 2019.

143 P. Grother, N. Ngan and K. Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', NIST report, December 2019.

144 P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer and C. Busch, 'Demographic bias in biometrics: A survey on an emerging challenge' IEEE Transactions on Technology and Society, 1(2), 2020, p. 98.

145 G. González Fuster, Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights, study for the European Parliament, July 2020.

146 European Citizens' Initiative, Civil society initiative for a ban on biometric mass surveillance practices, date of registration: 7 January 2021, deadline: 1 May 2022.

147 eu-LISA, Artificial Intelligence in the Operational Management, 2020.

148 Renda et al., Study to Support an Impact Assessment, 2021. p. 24.

149 B. Agüera y Arcas, M. Mitchell and A. Todorov, 'Physiognomy's New Clothes, Medium', 7 May 2017.

'phrenological impulse,'[150] where 21st-century computers and algorithms replace 19th-century cranial callipers and composite photographs.[151]

To help people understand and reflect on how computers can be used to detect emotion from facial expressions, researchers from Cambridge University and University College London built an interactive website called Emojify.[152]

Proposal for an artificial intelligence act

In April 2021, the European Commission put forward a proposal for an artificial intelligence act, which would classify AI systems used in the fields of migration, asylum and border control management as high-risk. High-risk systems will need to meet certain mandatory requirements concerning the quality of data sets used; technical documentation and record keeping; transparency and the provision of information to users; human oversight; and robustness, accuracy and cybersecurity. Recital 39 of the proposal refers explicitly to such AI systems:

AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools or to detect the emotional state of a natural person; for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council 49, the Regulation (EC) No 810/2009 of the European Parliament and of the Council 50 and other relevant legislation.

Source: European Commission, 2021.

7.2.2. Data protection and privacy

While most AI applications pose challenges of privacy and data protection, face recognition systems are particularly risky because of their capacity to identify individuals at a distance, in real-time or based on historical images or videos, even without the awareness of the individual. Paradoxically, the fact that the technology can be used remotely and with limited personal involvement seems to be one of the reasons why face recognition is generally preferred to other biometrics (though, in the case of fingerprints, this may be due to their association with suspicions related to crime).[153]

[150] Crowford, 'Time to regulate AI', 2021.

[151] L. Stark, 'Facial recognition is the plutonium of AI', XRDS: Crossroads, March 2019.

[152] https://emojify.info/menu

[153] Israel, 'Facial recognition at a crossroads', 2020, p. ii.

Whereas a lot of attention has been paid to curtailing the bias of AI applications, risks to fundamental rights remain and may even amplify, when technologies work as intended. For example, perfectly accurate and unbiased AI systems still pose significant data protection and privacy risks and appropriate measures are needed to address these risks.

The potential for 'covert, remote, and mass capture and identification of images'[154] creates serious privacy risks for individuals and threatens to transform the way in which people understand and experience public space. Critics have pointed out that mass surveillance initiatives relying on face recognition create a 'perpetual line-up' where citizens are treated as suspects.[155] In the context of EU borders, it is argued that new face recognition systems may further contribute to 'automating suspicion'[156] in regard to third-country nationals.

Whereas borders constitute a specific legal context allowing for certain legitimate limitations of fundamental rights safeguards, there is a risk that technologies adopted at the borders may be extended to other contexts (surveillance creep), without proper assessment.[157]

With regard to AI tools for migration monitoring, in 2019, the EDPS issued a temporary ban[158] on the production of social media monitoring reports by EASO due to the lack of a clear legal basis and 'serious data protection concerns', including about the lack of fairness and transparency of data processing and the potential chilling effect (force used to self-censor their online activity).

7.2.3. The risk of unlawful profiling

Technological advances allowed the development of profiling algorithms that rely on correlations and patterns in data. Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4) of the GDPR). Profiling is a legitimate tool used by law enforcement officers and border guards to prevent, investigate and prosecute criminal activity, as well as to prevent and detect irregular immigration.

Article 11 of the Law Enforcement Directive (LED) prohibits decisions based solely on automated processing, including profiling 'unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and

EU data protection safeguards

The General Data Protection Regulation (GDPR) provides for data protection safeguards regarding the processing of personal data, including biometric data.

People's facial images constitute biometric data within the scope of the EU data protection law. However, according to Recital 51 of the GDPR: 'The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person'.

The processing of personal data in the context of law enforcement and borders is regulated by Directive 2016/680, (Law Enforcement Directive).

[154] J . Lynch, 'Face-Off Report', Electronic Frontier Foundation, April 2020, p. 7.

[155] C. Garvie, A. Bedoya and F. Jonathan, 'The perpetual line-up: Unregulated police face recognition in America', Center on Privacy & Technology at Georgetown Law, 18 October 2016.

[156] Jones, 'Automated suspicion', 2020.

[157] Israel, 'Facial recognition at a crossroads', 2020.

[158] EDPS, Letter concerning a consultation on EASO, 2019.

freedoms of the data subject, at least the right to obtain human intervention on the part of the controller'. Profiling based on special categories of data,[159] including biometric data for the purpose of uniquely identifying a natural person, is exceptionally allowed if adequate fundamental rights safeguards are put in place and if it does not lead to discrimination.

The increased use of biometric data in EU information systems poses the risk of discriminatory profiling. For example, facial images (and even fingerprints) may reveal ethnic origin and could lead to automated ethnic classification.[160] Even when profiling is not based directly on special categories of data, it may use information that indirectly reveals such data. For example, in the context of the revision of the VIS, the FRA pointed out[161] that the use of 'current occupation' as a risk indicator may lead to discrimination based on prohibited grounds. This could be the case when members of a national or ethnic minority or people of certain nationalities are predominantly involved in a certain profession in a particular area, as opposed to the members of the majority. While ETIAS and PNR legislation prohibit basing risk indicators on criteria that entail a high risk of discrimination (such as race, ethnic origin or religious beliefs), these characteristics might be correlated with or inferred from other types of data. For example, information about a traveller's dietary preferences recorded in the 'general remarks' category of the PNR could be taken to reveal a traveller's religious beliefs.[162] Moreover, 'excessively broad criteria' used for risk assessment could lead to a significant number of false positives, meaning that persons are wrongly matched with a certain risk profile.

The automated processing of PNR data was a key issue raised by the ECJ in its opinion[163] (requested by the European Parliament) on the EU PNR agreement signed with Canada. The ECJ found that the agreement did not include sufficient fundamental rights safeguards, given that the Canadian pre-established models and criteria used for the automated processing of PNR data could result in individual decisions with binding effects, 'without there being reasons based on individual circumstances that would permit the inference that the persons concerned may present a risk to public security'. Two other requests for preliminary rulings related to the compatibility of the EU PNR Directive with EU fundamental rights are pending before the ECJ.

One safeguard provided by the Law Enforcement Directive in the context of profiling is the right to obtain human intervention on the part of the controller (Article 11). Such a 'human in the loop'-safeguard, however, may be weakened in practice by automation bias – the fact that human operators tend to defer to automated systems (especially when in doubt) when taking decisions.[164]

Another safeguard concerns the right of data subjects to receive an explanation of the decision. Such a right to explanation, which is mentioned only in the recitals of the GDPR and the LED,[165] has been intensely debated in association with opaque AI applications (black boxes). Given that there

[159] Special categories of data refer to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person's health, sex life or sexual orientation.

[160] FRA, Fundamental rights and the interoperability of EU information systems: borders and security, 2017.

[161] FRA, The revised Visa Information System and its fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights, August 2018, p. 79.

[162] FRA, Preventing unlawful profiling, 2018, p. 117.

[163] ECJ, Opinion of the Court (Grand Chamber) of 26 July 2017.

[164] L. L. Skitka, K. L. Mosier and M. Burdick, 'Does automation bias decision-making? International Journal of Human-Computer Studies', *International Journal of Human-Computer Studies*, 51, 2019.

[165] GDPR, recital 71: the right ... to obtain an explanation of the decision reached"; LED, recital 38: 'right to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision'.

are no explicit legal provisions on this right to an explanation or any relevant jurisprudence, the scope of this right remains unclear.[166]

7.2.4. Transparency in EU research funding on AI

One issue that transpired in the controversy around the iBorderCtrl project is about the transparency standards in relation to EU funding for AI research. Patrick Breyer MEP filed a transparency complaint[167] before the ECJ against the European Research Executive Agency for its refusal to disclose specific documents related to the project. In response to a parliamentary question, the Commission stated[168] that 'iBorderCtrl was a research project and did not envisage piloting or implementing a working system' and that any future decision on the use of the results will take into account the 'scientific reliability and political, societal, ethical and financial implications', as well as the need for compliance with the applicable EU law.

As described in the Horizon 2020 manual,[169] 'ethics is an integral part of research from beginning to end' and the ethical dimension of activities funded by the programme are assessed through an ethics appraisal procedure. However, according to a 2020 study,[170] there is a need for stronger transparency, oversight and accountability requirements with regard to EU funding for AI research (for instance, AI research on security) that may have a serious impact on EU fundamental rights.

8. Final reflections on (AI) technology

Discussions about AI, in particular in the media, often appear as a passionate battle between pessimists who see AI as a tool of destruction and optimists as a tool of salvation. If there is one thing that both camps seem to agree upon, it is that AI technologies are powerful tools that will have significant consequences across many domains. The danger, however, is to assume that, given the disruptive power of these technologies, it is *inevitable* that they will have such and such consequences, regardless of what we may do about it.

This kind of technological determinism may block a serious debate from being held about whether and how technologies should be developed and adopted. For example, claiming that emotion recognition is possible and declaring that technologies based on it are 'the future' of border and security checks does not say much about the desirability and acceptability of such technologies. A hint at such deterministic tendencies can be detected in a recent eu-LISA report,[171] which states that the implementation of AI is not a question of 'if', but 'when' and 'to what extent'. Two researchers made an interesting analogy between the current rush to adopt digital technologies and the way humanity has addressed previous technological challenges: the fact that cars can run at 250 kilometres an hour has not stopped regulators from imposing driving speed limits for reasons of public safety. In other words, 'just because some technologies are possible, it does not mean that they should be accepted'.[172] The international agreement on the non-proliferation of nuclear

166 FRA, Fundamental rights and the interoperability, 2017, p. 44; For a more detailed discussion, see G. Sartor, The impact of the General Data Protection Regulation (GDPR) artificial intelligence, study, EPRS, European Parliament, June 2020.

167 ECJ, *Breyer v REA*, Case T-158/19.

168 Parliamentary question, Answer given by Ms Johansson on behalf of the European Commission, 24 February 2020.

169 European Commission, Funding & tender opportunities, Ethics.

170 González Fuster, 'Artificial Intelligence and Law Enforcement', July 2020.

171 eu-LISA, Artificial Intelligence in the Operational Management, 2020, p. 32.

172 E. Mendos Kuskonmaz and E. Guild, 'Covid-19: A New Struggle over Privacy, Data Protection and Human Rights?', *European Law Blog*, 4 May 2020.

weapons is another example of a successful attempt to regulate how powerful yet highly destructive technologies should be used.

It is a well-established view in technology- and society-related studies that technologies are not 'just' technologies, divorced from the social, political and cultural contexts in which they are developed and deployed. For example, the current development of face recognition technology is not solely driven by the pace of scientific research but is also embedded in the 'securitisation of identity' and surveillance culture of the last two decades.[173]

The development and implementation of technologies is often seen as a series of purely technical adjustments and improvements. Such a view may contribute to attributing a false sense of objectivity to technologies, in which technological changes become dissociated from the broader legal, social and ethical issues they (most likely) pose. This false perception is reinforced both by the way technologies work and the way humans take decisions and interact with technologies. In the case of data-driven AI technologies, their opacity and complexity (the common 'black box' objection) make it difficult to scrutinise and challenge the results.[174] The complexity of technologies and the increasing automation of tasks may lead to automation bias. Moreover, exaggerated claims about the accuracy level of technology may create a sense of over-confidence in the results among officials.[175]

Neither the design nor the operation of algorithms constitutes a purely technical, neutral activity. Yet, many decisions concerning algorithm design and optimisation (such as weighting probabilities, sensitivity and accuracy thresholds) happen behind the scenes and are often relegated to (IT) experts.[176] However, in many cases, 'technical' decisions require dealing with and striking a balance between conflicting values, norms and interests (e.g. data protection versus security). This raises the question of accountability (who decides?).

Lastly, a full understanding of the issues raised by AI technologies would benefit from a longer-term perspective. Many 'new' technologies may prove to have revealing and sometimes unexpected historical and intellectual roots. For example, attempts to identify and classify people according to their physical characteristics, in particular their faces, have a long and troublesome history. While AI researchers and promoters may not (all) be secret physiognomists (trying to detect people's personality and criminal traits through their facial features), the failure or unwillingness to question problematic assumptions built into or associated with particular technologies does not make the impact of these technologies less harmful.

173 Gates, 'Our biometric future', 2011.

174 W. Knight, 'The Dark Secret at the Heart of AI', *MIT Technology Review*, 11 April 2017.

175 Israel, 'Facial recognition at a crossroads', 2020, p. v.

176 L. Amoore, 'Doubt and the algorithm: On the partial accounts of machine learning', *Theory, Culture & Society*, 36 (6), 2019.

The EU is actively exploring how AI technologies can be developed and adopted in order to improve border control and security. A number of applications for biometric identification, emotion detection, risk assessment and migration monitoring have already been deployed or tested at EU borders.

AI technologies may bring important benefits for border control and security, such as increased efficiency, better fraud-detection and risk analysis.

However, these powerful technologies also pose significant challenges, related in particular to their insufficient or varying accuracy and the multiple fundamental rights risks they entail (including bias and discrimination risks, data protection and privacy risks, and the risk of unlawful profiling).

QA-08-21-191-EN-N

This is a publication of the Members' Research Service
EPRS | European Parliamentary Research Service

PE 690.706
ISBN 978-92-846-8363-5
doi:10.2861/91831