AI in Border Control and Surveillance.

Current and Future implications

Large Scale Biometric Databases

Two Decades of Developments (2000s - Present)

These extensive repositories of biometric data, such as fingerprints and facial images, have become the backbone of border security. Over the years, these databases have evolved, granting law enforcement access and even proposing expansions to include more data points.

2000

- Biometric registration of asylum-seekers.
- Establishment of the Eurodac database to store asylum-seekers' fingerprints.
- Intended to aid in determining the state responsible for processing asylum applications.

2011

- EU biometric visa database (VIS) comes into use.
- Full global deployment completed by the end of 2015.

2013

- Fingerprints and photographs added to the Schengen Information System (SIS).
- Legal changes introduced alerts on deportation orders in SIS.

2015

- European Commission "non-paper" calls for a 100% fingerprinting rate in Eurodac.
- Argues "no registration no rights."

2016

- Legislation proposed to make Eurodac a general-purpose "migration management" database.
- Proposal includes facial images, biographic data, and inclusion of more groups of people.

2017

- Entry/Exit System (EES) legislation introduced.
- EES will monitor the cross-border movements of temporary visitors to the Schengen area.
- It aims to replace manual passport stamping with a centralized database containing biometric and biographic data.

2018

- Approval of the "travel authorization" system, known as the European Travel Information and Authorization System (ETIAS).
- ETIAS will require non-EU citizens who do not require a visa to pay for a "travel authorization."

2020

- Legislation interconnecting all EU migration and policing databases.
- "Interoperability" architecture to take "identity data" from five large-scale EU databases and place it in a new Common Identity Repository.

Surveillance and Data Infrastructure

Advancements from early 2000s to present

The intricate web of surveillance tools, data-sharing mechanisms, and pre-frontier situational awareness systems.
Airlines transmitting passenger information, interconnected surveillance assets, and efficient case management systems play crucial roles in enhancing border security and situational awareness.

01 - Advance Passenger Information (API) (2004): Airlines transmit passport information to EU border authorities for pre-checks against immigration databases.

02 - European Border Surveillance System (EUROSUR) (2008): EUROSUR interconnects national and EU surveillance assets, incorporating drones, cameras, and sensors to enhance border surveillance and provide pre-frontier situational awareness.

03 - Readmission Case Management Systems (RCMS) (2013): These systems facilitate communication between deporting and destination states, exchanging information for identity verification and deportation procedures.

04 - Passenger Name Record (PNR) Directive (2014): PNR data is used for 'pre-checks' against airline passengers for policing purposes.

05 - Automated 'Lie Detectors' (2014): Innovative systems like AVATAR and iBorderCtrl aim to examine travelers' gestures and expressions for irregular behavior.

06 - Frontex sharing of migrants' personal data (2015 onwards): through projects like PeDRA, Frontex collects personal data from migrants to be shared with Europol for risk analyses.

Artificial Intelligence at Borders

Navigating Future Developments and Concerns

A 2020 study for the European Commission explored ways to integrate AI in border control, migration and security. The study proposes a roadmap listing different forms of AI technology for EU border control

Chatbots

AI-powered chatbots could be used in online application processes for long-term stay or migration in the Schengen area as well as permission to move to another EU member state. They could provide real-time information, answer queries, and streamline border crossing procedures.

Risk Assessment Tools

AI could also be used to "triage" applications, determine which require a more thorough risk analysis, speed up risk assessments and background checks. However, they raise important concerns on risks of "inadvertent racial bias" and discrimination.

Computer Vision

AI's computer vision capabilities are harnessed to analyze imagery for anomalies, strenghtening border surveillance. These systems can detect irregularities in vehicle cargo, monitor border areas with drones, and even identify forged documents through image analysis.

While AI aims to streamline migration and border management and enhance security, automating the asylum process with AI may worsen its dehumanizing aspects in an already flawed system.

Surveillance Technologies Landscape

Emerging Technologies and Risks

A 2022 study by the European Commission and Frontex identifies 11 distinct surveillance technologies of interest. These range from drones and intelligent video surveillance to algorithmic tracking systems.

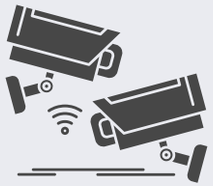
FIRST PRIORITY TECHNOLOGIES

High Altitude Pseudo Satellites (HAPS)

High-flying platforms for persistent border surveillance.

Real-time data collection from connected border infrastructure.

Internet of things (IoT)



Intelligent Video Surveillance

AI-driven cameras for automated threat detection.

Long-range object detection in all weather conditions.

Radar Technologies

Underwater Sensors

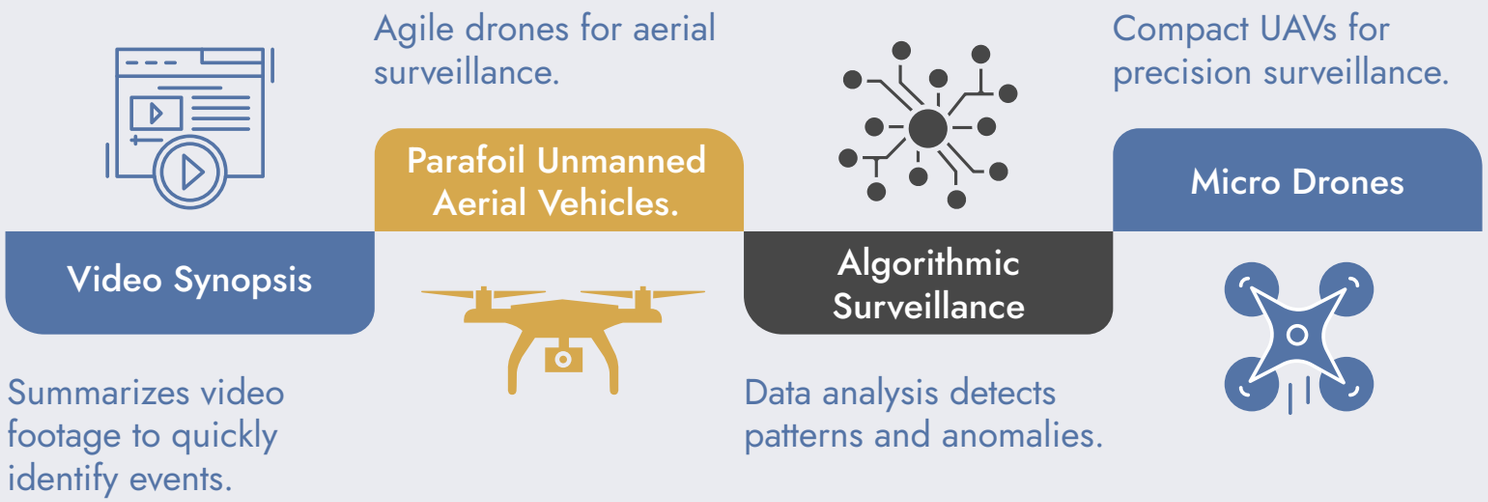
Sonar-based monitoring for underwater border crossings.

These technologies bolster border security but also raise pressing concerns about privacy, data protection and fundamental rights.

Surveillance Technologies Landscape

Emerging Technologies and Risks

SECOND PRIORITY TECHNOLOGIES



These technologies bolster border security but also raise pressing concerns about privacy, data protection and fundamental rights.

Biometrics Unveiled

Exploring Future Potential and Associated Risks

A 2021 study by Frontex, identified five key technology clusters with the greatest potential for influencing border management practices. Notably, these clusters include advancements like contactless friction ridge recognition and 3D face recognition.

01

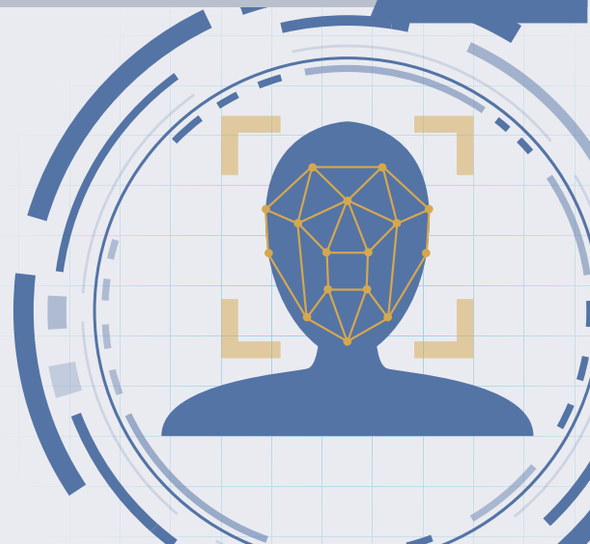
Contactless Friction Ridge Recognition: This technology captures distinctive patterns from fingers, palms, feet, or finger-knuckles without physical contact. While not currently used in border checks, it holds the promise of recognizing individuals even from a short distance. Future applications may enable stand-off person recognition, from several meters away.

02

3D Face Recognition: Unlike traditional 2D face recognition, 3D face recognition employs the three-dimensional features of a person's face for automated recognition and matching. It extracts unique features from the face's surface geometry, offering potentially higher accuracy.

03

Infrared Face Recognition: This technology utilizes various infrared technologies, including thermal and near-infrared, to capture and scan faces. It performs biometric matching against infrared images stored in databases. It's known for its impressive presentation attack detection capabilities and relative ease of capturing infrared images.



04

Iris Recognition in the NIR Spectrum: Iris recognition in the near-infrared (NIR) spectrum is highly accurate and contactless. It captures the unique features of the iris without physical contact, making it efficient and secure. It can also be performed from a distance, even for individuals in motion.

05

Iris Recognition in the Visible Spectrum: This technology relies on visible light to capture images of the iris. While it displays good capability readiness from 2028 onwards, it faces challenges with individuals who have dark irises due to reduced visibility of unique iris patterns under visible light.

Privacy and Rights Considerations

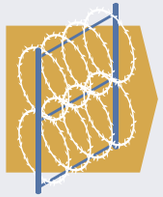
The integration of AI and surveillance raises significant considerations at the intersection of technology, privacy, and human rights. Exploring these concerns is crucial to strike a balance between security and safeguarding fundamental freedoms.

PRIVACY

The proliferation of surveillance technology amplifies data collection efforts, posing potential threats to individuals' privacy. The extensive gathering of personal information and its storage demand robust data protection measures to mitigate risks.

FREEDOM

Efforts to enhance security should be carefully balanced with protecting personal freedoms. Ensuring that surveillance practices do not infringe on individual rights to privacy, freedom of movement, and freedom of expression remains a critical challenge.



ASYLUM

The integration of surveillance technologies can have implications for individuals seeking asylum. It's imperative to consider how these technologies might impact the right to seek asylum, ensuring that those in need can access protection in accordance with international law.

HUMAN RIGHTS

Preserving human rights is crucial in this context. Striking a balance between security measures and these fundamental rights, such as the right to life, liberty, and non-discrimination, presents an urgent challenge.

Conclusion

Reflecting on the EU's technological evolution for border management, it's evident that advancements in biometrics, surveillance, and artificial intelligence have reshaped border control. These innovations promise enhanced security and efficiency, but they also bring forth pressing concerns. Balancing security with privacy, safeguarding human rights, and ensuring responsible technology transfer are paramount as the EU navigates this dynamic landscape. The path ahead must prioritize the preservation of fundamental rights, individual freedoms, and regional stability.

EuroMed Rights would like to thank the European Artificial Intelligence & Society Fund whose support enabled this research.
The sole responsibility for the content lies with the author(s) and acontent may not necessarily reflect the positions of NEF, or the Partner Foundations.

European Artificial Intelligence & Society Fund

September 2023
Tel: +45 32 64 17 00
information@euromedrights.net
www.euromedrights.org

DROITS EUROMED RIGHTS