INTERNET POLICY REVIEW

Volume 13 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Navigating data governance risks: Facial recognition in law enforcement under EU legislation

Gizem Gültekin-Várkonyi *University of Szeged* gizemgv@juris.u-szeged.hu

DOI: https://doi.org/10.14763/2024.3.1798

Published: 30 September 2024
Received: 22 February 2024 **Accepted:** 6 August 2024

Funding: The research was supported by the ICT and Societal Challenges Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.
Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/3.0/de/deed.en
Copyright remains with the author(s).

Citation: Gültekin-Várkonyi, G. (2024). Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1798

Keywords: Data protection, Facial recognition software, Biometric, Law enforcement, Policing

Abstract: Facial recognition technologies (FRTs) are used by law enforcement agencies (LEAs) for various purposes, including public security, as part of their legally mandated duty to serve the public interest. While these technologies can aid LEAs in fulfilling their public security responsibilities, they pose significant risks to data protection rights. This article identifies four specific risks associated with the use of FRT by LEAs for public security within the frameworks of the General Data Protection Regulation and Artificial Intelligence Act. These risks particularly concern compliance with fundamental data protection principles, namely data minimisation, purpose limitation, data and system accuracy, and administrative challenges. These challenges arise due to legal, technical, and practical factors in developing algorithms for law enforcement. Addressing these risks and exploring practical mitigations, such as broadening the scope of data protection impact assessments, may enhance transparency and ensure that FRT is used for public security in a manner that serves the public interest.

This paper is part of **AI systems for the public interest**, a special issue of *Internet Policy Review* guest-edited by Theresa Züger and Hadi Asghari.

1. Introduction

Technology has revolutionised law enforcement, evolving from automated fingerprint systems to sophisticated crime prediction tools (Hoey, 1998). Law enforcement agencies (LEAs) now leverage big data and facial recognition technologies (FRTs) to process vast amounts of biometric data for law enforcement purposes, including facial features and retinal patterns, collected via tools like CCTV cameras, drones, and online platforms. FRT primarily handles biometric data that is diverse, such as facial features and retinal patterns, linking them to the purpose of FRT which is to use them for identifying individuals (European Data Protection Board, 2023). In the US, 30 million cameras record 4 billion hours of footage weekly, potentially used for monitoring activities like riots (Hodge, 2020; USGAO, 2021).

FRTs usually have the potential to enhance public safety, security, and justice, aligning with the United Nations Sustainable Development Goals (Chui et al., 2018; Shi et al., 2020). For example, FRTs are employed at the Schengen Area's external borders to enhance the security and integrity of immigration procedures.[1] Because it is used by border authorities for a very specific purpose (to monitor and control the crossing of a land border), at a specific time (when an individual is attempting to cross the border), and in a specific place (a border crossing point), it may serve to establish a level of trust between the public (the trustor) and the authorities (the trustee), despite the lack of empirical evidence. Nevertheless, such a specific use increases the likelihood that the negative impact on fundamental rights will be minimal and that identifiable risks can be partially mitigated. In this way, it is an opportunity for LEAs to ensure safe migration, which is one of the elements of public security that falls under the broader public interest.

The debate over whether FRT genuinely enhances public security and serves the public interest persists. This is primarily because FRTs also pose significant surveillance risks, with studies showing public perceptions about increased surveillance despite recognising FRT's crime prevention potential (Pew Research Center, 2022; Kostka et al., 2023; Lyon, 2002). One reason surveillance may proliferate is due to

1. External borders of the Schengen area is defined in the Article 2 of the 2016/399 Schengen Borders Code as "Member States' land borders, including river and lake borders, sea borders and their airports, river ports, sea ports and lake ports, provided that they are not internal borders".

violations of data protection and privacy rights, stemming from the continuous and varied use of FRT (De Cremer, 2020; Floridi et al., 2020). Data collected through FRT can be used to create comprehensive profiles of individuals, including indicators of potential criminality or even categorisations of groups with similar identities (Delikat, 2021; EDPB, 2023). Automatic profiling often not only limits individuals from expressing themselves or correcting potentially inaccurate categorisations but also raises concerns regarding the unintended purposes of the technology, which can lead to public distrust. Such limitations complicate individuals' efforts to understand, contest, and rectify erroneous or biased decisions (Palmiotto, 2024), therefore decreasing the reliability of the system's purpose of operation to serve the public interest.

In the EU, the GDPR and the AIA primarily govern biometric data processing through FRTs.[2] The GDPR ensures lawful data processing, while the AIA aims to create trustworthy AI based on such data.[3] Biometric data is classified as special personal data under the Article 9 of the GDPR, with processing allowed only in exceptional cases, such as for public security. Article 5 of the AIA classifies biometric data processing tools under the category of high-risk AI systems meaning that the placement of such tools in the market is possible under strict rules. Furthermore, real-time biometric data processing tools in publicly accessible spaces for law enforcement purposes are classified under the category of unacceptable risk which means that their operation is generally prohibited, except where they serve limited purposes. Obviously, both legislations permit biometric data processing and tools for law enforcement purposes with considerable discretion in interpreting rules regarding public security. Even though use of FRT by LEAs under the AIA will be possible under some heightened safeguards and within the guidance of the interpretation of national authorities of the member states, at LEAs in the interim period between the introduction of the AIA and the first interpretations from the national authorities arrive, LEAs will need to interpret rules on processing biometric data for law enforcement purposes independently. Even after that, the legal, technical, and practical aspects of deploying FRT could lead to breach of data protection rights, affect uniform application of the GDPR and the AIA, and cause inconsistencies during implementation. For this reason, human rights organisations criticised the removal of the proposed general ban on real-time FRTs as outlined in the draft

2. The article leaves an in-depth analysis of the Law Enforcement Directive for future consideration since the evaluated risks in the article are clearly in common between the GDPR and the LED.

3. Trustworthy AI is the cornerstone of the AIA, as it aims the acceptance and effective use of these systems to be contingent upon the trust of all stakeholders, such as the LEA. See, Recital 59 of the AIA emphasising the importance of ensuring that AI systems used by law enforcement are accurate, reliable, and transparent to maintain public trust and uphold fundamental rights.

AIA text of June 2023, as well as the final text, which they found to include insufficient restrictions on FRT use. They argued that these provisions undermine privacy and exacerbate public concerns regarding the balance between security and privacy (EDRi, 2021; EDRi, 2023; EDPS, 2021; Amnesty International, 2023).

This article examines four potential risks posed by FRT in law enforcement, focusing on legal, technical, and practical aspects under the GDPR and AIA. If not carefully evaluated, these risks can erode public trust, undermining the public interest LEAs aims to protect (Mazzucato, 2022) by providing insufficient scrutiny power to individuals to defend their data protection rights. Notably, aside from the GDPR and the AIA, which partially regulate FRT implementation, there is currently no specific legislation in Europe governing FRTs, particularly their application in law enforcement (Mobilio, 2023). The risk analysis presented here is to highlight the gaps and aims to propose a tech-by-tech approach to extending the scope of implementation of existing legislation to FRTs in law enforcement. The expansion of data protection impact assessments to FRTs' applications, their adoption as part of the decision-making process, and their integration into a wider risk management scheme introduced by the AIA could contribute to lawful use of FRT for public security purposes.

2. FRTs' diverse applications

In order to engage in discourse surrounding FRTs, it is first necessary to define the term. This is a challenging task given the lack of a universally accepted definition. The extant research and legal discourse present a multitude of technical and legal interpretations of FRT, each emphasising different aspects. For example, from a legal perspective, as seen in the AIA, FRT is conceptualised primarily through its role in biometric data processing, as will be presented in the definitional challenges title of this article later. On the technical side, for instance, Selwyn et al. (2024) emphasise the various functions of FRT, such as facial processing, categorization, and analysis, with each technique being specific to its intended use. Despite the absence of a universally accepted definition of FRT, all definitions converge on a common focus: the purpose of use. This approach aims to reduce the ambiguity surrounding the term and address the issue of the lack of a standardised definition. Nevertheless, while the purposes of using FRT can sometimes be unclear, the associated risks are not, as Akbari (2024) stated. This means that from a risk assessment perspective, it is the intended use, not only the definition, that determines the risk. The purpose of use shapes the definition, and as the purpose changes, the risks change accordingly.

FRT serves various purposes, such as face recognition, emotion and behaviour assessment, and individual tracking in crowds (Gillis et al., 2021). These purposes can be classified into three main categories with each point a function: authentication, identification, and profiling. In law enforcement, one or multiple functions could be operated, and the discernment of functionality and purpose remains pivotal for comprehensive risk assessment (Christakis et al., 2022b). The methods used to develop FRT algorithms typically reveal their intended function and purpose. For instance, a one-to-one search method is employed for authentication purposes, such as unlocking a mobile phone with a facial identification tool. One-to-many search in airports is used to identify individuals and allow them to cross the border. These methods rely on a query to a database of known individuals and work post-biometric processing. The many-to-many search method used in live biometric processing activities is particularly noteworthy due to the heightened risks it introduces.[4] This has the potential to be used for surveillance purposes on anyone, anywhere, and at any time. Surveillance purposes here could include not only recognising someone, but classifying them according to their age, gender, or race, or even further categorising them according to how they feel. According to a study, out of the 27 EU member states, 11 currently employ FRT, with the one-to-many method being commonly used by the LEAs (TELEFI project, 2021). In Europe, the Metropolitan Police Service in London has a track record of employing live FRT that was developed using a many-to-many method (Mansfield, 2023). Nevertheless, despite its ability to process a facial image with a time delay of a few seconds, a live FRT is currently being used by police in the German eastern state of Saxony and in Berlin in the area of cross-border gang crime (Borak, 2024).

According to the ICO (2021), risks arise when the same functionality is used for different purposes and in different settings, or when the same purpose could be served by different functionalities. Christakis et al. (2022b) note that when combined with techniques such as predictive policing, FRT becomes even riskier as it combines the potential risks of two different systems. This could go beyond the mere public security purpose to lifelong surveillance. From the legal point of view,

4. The differentiation between these methods can be explained as follows: One-to-one method involves comparing one known facial image to another single known facial image in the facial image database. It is used to verify if two images represent the same individual, such as unlocking a building's door with facial verification.The AIA uses these terms in the definition of biometric verification. One-to-many method involves comparing one known facial image to many facial images in a database. It is used to identify an individual by finding the closest match among many stored images, for example, identifying a missing person from a database of found individuals. Many-to-many method involves comparing multiple unknown facial images to many facial images in a database. It is used to match groups of images to each other, which can be applied in large-scale surveillance to identify multiple individuals within a crowd at a large public event. See USGAO, 2021 for more insight.

the GDPR does not differentiate between the methods mentioned technically (Kindt, 2020, pp. 62-69), which creates uncertainties particularly for providers who focus mostly on the technical aspects of FRT in their efforts to ensure public security. Further, as the methods also give some ideas on the purposes, the risks arising from specific uses of FRT differ. Similarly, LEAs may struggle to comply with the law because they may not always be aware of the technical perspective of the providers. Failure to adhere to legal and ethical standards by the key stakeholders involved in FRT operations is likely to undermine public trust and acceptance, as will be shortly discussed below. Technical complexities, coupled with legal ambiguities, pose significant challenges to upholding fundamental principles outlined in the legislation, such as purpose limitation, data minimisation, data accuracy, and administrative constraints. Each of these factors plays a crucial role in transparently communicating the intended purpose of FRT deployment to the public. The GDPR, like the AIA, avoids regulating specific technologies and instead establishes a general framework. However, as AI advances and becomes more specialised, the associated risks will increasingly target specific sectors. Therefore, a technology-specific approach to risk assessment should have been considered by the EU lawmaker, even though this is now challenging to implement. Nonetheless, it is crucial to emphasise the need for targeted risk assessments for FRTs, as existing legal tools offer guidance on addressing specific technologies.

3. Intersection of trust, risk, and FRT for public security

In order to ascertain whether a risk-based approach can be applied to a specific technology and its correlation to public trust, it is first necessary to see the relationship between the relevant terms. The concept of public trust represents a fundamental pillar of public interest, as it serves to reinforce the conviction that institutions are committed to safeguarding the collective interests of the community, such as public security which is the main focus of this article. The effective management of these areas is entrusted to state authorities with the objective of safeguarding the social good. Simply, a lack of public trust in authorities represents a significant challenge to the foundations of democratic systems, human rights, and the rule of law. The legal framework defines the scope of public interest, though is not an ambiguous term, and the extent to which the state is permitted to protect these interests. Through the consent and trust of the governed, the state is authorised to protect these interests through legal tools. This section will present the inconclusive outcomes observed in the literature with regard to the positive or negative correlation between public trust and a specific technology targeting to ensure public security. This understanding then provides the basis for evaluating

the use of FRT under the GDPR and the AIA from the risk assessment perspective.

The term trust is inherently ambiguous, defined through various dimensions at both individual and public levels. At the individual level, trust stems from psychological, cognitive, rational, or emotional factors, influencing public trust. Trust is contingent on aligned interests, where mutual expectations of trusted and trustee play a crucial role (Hardin, 2001). Palmisano and Sacchi (2024) argue that trust depends on perceptions of uncertainty or risk, with the example of education reducing risk-taking tendencies. Degli-Esposti and Arroyo (2021) highlight that control mechanisms like transparency are essential in fostering public trust in technology by mitigating risk. Hence, trust and risk are interrelated, affecting both interpersonal and technological contexts.

In the context of FRT used for public security, assessing the trust between the public and deployers (particularly LEAs and providers) is crucial to determine if the technology meets its intended security goals. Various studies explore public trust in LEAs, some linking it to governance processes (UNDP, 2021), and many attempts to measure it via public surveys. These surveys, however, reveal mixed results: some studies suggest that trust enhances positive attitudes towards surveillance, while others argue that surveillance undermines trust (Herreros, 2023). For instance, the Police Barometer study shows that 90% of Finns trust their police due to effective emergency operations and fair decision-making (Vuorensyrjä et al., 2023). However, some scholars criticised the complexity of the parameters used in these surveys and highlight a lack of theoretical rigour (Kääriäinen, 2008; Björklund, 2021). Thus, existing literature provides only descriptive insights into the trust-LEA-technology relationship, often failing to confirm its validity. Further, researchers suggest that factors like ethnic diversity, religious groups, education levels (Palmisano and Sacchi, 2024), police treatment of minorities (Valentin, 2019), and trust in justice and institutions (Hough et al., 2013) influence public trust. Procedurally fair treatment, including police interactions and language use, also affects trust (Murphy, 2013). Presumably, it is impossible to consider all these factors simultaneously when evaluating potential risks, however, identifying who benefits most from the FRT should highlight potential imbalances and inform more precise risk assessments.

3.1 Who benefits most and at what risk?

FRT tools for security use present both advantages and disadvantages that can impact public trust in these technologies and their deployers. Clearly defining the purpose, target, and duration of their use can help mitigate public distrust towards

LEAs. When used specifically for identification or verification rather than widespread monitoring, FRT has the potential to enhance security in targeted scenarios, thus aligning with public interest by contributing to improved public security. For instance, individuals may perceive an enhanced sense of security due to the monitoring of perpetrators of criminal acts such as bank robberies or acts of terrorism. FRTs can assist in identifying individuals whose documentation is lost in disasters and in identifying victims of war and disasters (Selwyn, et al., 2024). In healthcare, FRTs aid medical professionals in rapidly identifying novel diseases, such as during COVID-19 they helped understand the virus's spread by providing statistical data (Fontes et al., 2022). According to Solarova et al. (2022), people are more likely to accept FRTs if they believe it is genuinely for security purposes and limited to that context. In private use, FRTs could make life easier, such as through online secure payments.

However, when surveillance enters the picture, FRT appears more beneficial for LEAs and providers than for the public. Moy (2021) posits that manual identification from camera footage is time-consuming and labour-intensive. In protests, governments may use FRT to monitor participants rapidly and efficiently, while companies may sell data to the government, potentially reinforcing governmental power if there is insufficient oversight and accountability (Zalnieriute, 2024). This phenomenon, known as surveillance capitalism (Zuboff, 2019), exploits human experience for commercial purposes, enabling companies to influence citizen and government behaviour, potentially eroding democratic principles and individual autonomy. Some practices show that FRT can assist law enforcement in efficiently identifying and apprehending suspects (Hamann & Rachel, 2019). However, evidence supporting this is limited, as others suggest FRTs could lead to misidentification and wrongful convictions, reinforcing inaccuracies associated with eyewitness identification (Moy, 2021). Governments and providers may adopt advanced technologies despite significant risks, not only to facilitate their duties but also to conduct surveillance on people. For example, the FBI's FACE Services unit uses FRT to search driver’s licence databases, passport photos, and visa application photos, creating a biometric database of primarily law-abiding Americans without their knowledge (Garvie et al., 2016). While FRT offers potential for law enforcement, the absence of regulatory and practical evaluations reinforces existing risks, contributing to public distrust (Bragias et al., 2021). This raises questions about whether its use genuinely serves the public interest and whether the risks posed by surveillance technologies are worth taking.

3.2 Lower risks, better trust?

The relationship between risk, public trust, and public interest in the context of FRTs used by LEAs for public security is complex and debated. It is reasonable to assume that public acceptance of LEAs' services would increase if risks are effectively mitigated and clearly communicated. However, this does not guarantee unanimous support, as there is no consensus that risk mitigation alone will enhance public trust (Matulionyte, 2024). Historically discriminated groups by law enforcement may remain sceptical, despite claims of public security benefits. Still, risk management is a tool entrusted by law with the purpose of evaluation of the suitability of risky implementations. The AIA's risk management system may be designed with this goal in mind. The risks presented in this article focus on a selected few related to the processing of personal data with the aim of highlighting the importance of robust data governance frameworks.

4. FRT data governance in EU legislation

Algorithms begin and progress through their lifecycle by processing data, mostly personal data. While ongoing work is being done to develop techniques for creating well-performing algorithms with less data (Nguyen et al., 2023; Plangger et al., 2023), algorithms still require varying sizes and forms of data to function. Clearview AI is a FRT combined with a predictive policing tool developed by a private company and used by LEAs in several EU member states, including France, Belgium, and Italy. It holds approximately 30 billion images, mostly consisting of biometric data (Clayton and Derico, 2023). Biometric data is defined in the GDPR (Article 4, para.14), as the data generated through technical processes aimed at identifying or verifying the identity of individuals based on their physical, psychological, or behavioural characteristics. This definition distinguishes biometric data from other types of personal data by emphasising the importance of technical processes. In order for images to be classified as biometric data, they must be processed through a system that matches them with an individual's identity (Article 9 GDPR). According to the definition, either the data processed in the FRT or the output resulting from that processing is considered personal data. For instance, personal data includes the output of combining an individual's current psychological state, as revealed through facial images, with their past criminal record. The AIA follows the same approach as the GDPR in defining biometric data. This connection demonstrates that the risks associated with FRTs under the GDPR are also relevant to the AIA. These risks stem from compliance issues, legislation deficiencies, and practical implications that ultimately impact public opinion on the necessity of FRTs. By recognising and mitigating the risks outlined below, there is a

greater chance of achieving a balance between public security and privacy by enhancing transparency.

4.1 Risk one: Violation of general principles – data minimisation challenge

The use of FRTs in public spaces has the potential to violate individuals' rights to data protection which contradicts the general principles governing the processing of personal data outlined in the Article 5 of the GDPR, particularly the data minimisation rule. This rule has already been breached in practice, leading public authorities to intervene in terms of protecting public interest. The Italian DPA penalised Clearview AI's FRT tool, as they violated rules related to transparency and purpose limitation by collecting biometric and geolocation data without a proper legal basis (EDPB, 2022). Despite facing fines exceeding €20 million from various EU data protection authorities (Noyb, 2023), Clearview AI and similar companies continue to develop algorithms using unrelated data.

The principle of data minimisation is not only related to the protection of individuals but also to the protection of the public in general (FRA, 2018, p. 125). LEAs' wide range of data processing activities without explicit rules may cause fear of constant surveillance. As a result, pervasive surveillance significantly undermines individuals' autonomy, making them feel compelled to conform to expected behaviours in public spaces (Norris, 2002). These spaces are characterised by their accessibility to the general public, regardless of whether they are publicly or privately owned.[5] Public spaces are often referred to as "uncontrolled environments" (Consultative Committee, 2021, p.5), and the use of surveillance cameras means that individuals who pass by them become subjects of surveillance without any justification, leading to an environment controlled by authorities. Instead of freely expressing themselves, the knowledge of being watched forces people to conform to societal norms and expectations, thereby limiting their freedom and self-expression (Lyon, 2022). This is mainly because they often have limited knowledge about the fate of their data once it is captured by FRTs. Even if they were aware, they may face challenges in exercising their rights, such as the right to erasure under Article 17 of the GDPR or the right to restriction of processing of their data under Article 18 of the GDPR. When surveillance is targeted at a group, they have almost

5. Public spaces, as in form of publicly accessible space, are also defined in the Article 44 the AIA as "any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions". This definition encompasses a range of locations, including streets, shopping malls, city squares, airports, office buildings, theatres and further as listed in Recital 19 of the AIA.

no chance of escaping the surveillance, and they cannot collectively request their rights since the GDPR does not recognise collective rights. In 2018, police used live FRT to scan the faces of individuals participating in a peaceful protest in a public space in the UK. This action led to a legal case as everyone's face was scanned without being informed about possible algorithmic evaluation. As a result, the protestors felt unsafe when exercising their right to protest *(Bridges v CC-SWP,* 2019*)*. Despite the FRT deployed to enhance public security, its operation resulted in suppression of individuals, providing no tangible benefit.

4.2 Risk two: The challenge of limiting the purposes

The inherent nature of AI systems poses a significant challenge in terms of processing data, which diverges from the fundamental principle of processing personal data for a specific purpose (Article 5(b) GDPR). While biometric data may initially be collected for a specific purpose, AI algorithms can be trained to generate outputs that may suggest alternative purposes, such as using CCTVs installed in shopping centres for employee monitoring (EDPB, 2020) or identifying family connections and ethnicity, potentially leading to an Orwellian society. This functional shift, known as function creep (Koops, 2021), allows data to be processed beyond its primary purpose, which is permissible only under certain criteria, such as with the consent of the data subject (Article 6(1)(a) GDPR). However, consent practices can be deceptive,[6] particularly when used by LEAs. For instance, Clearview AI evaluated data not only for system development purposes but also for surveillance without individuals' consent (Rezende, 2020). This lack of transparency and individual agency underlines the power disparity between authorities and individuals, making it challenging for the public to assess risks or limit surveillance. Despite efforts by DPAs to intervene, such as the Swedish DPA penalising the Swedish police for using Clearview AI without specific purpose indication for surveillance (EDPB, 2021), technology evolves rapidly, outpacing regulatory responses to stop function creep. LEAs, as part of their public security responsibilities, are increasingly using advanced AI tools such as ChatGPT without obtaining individual consent and without informing the public (Europol, 2023). Additionally, techniques like soft biometry are being developed to assist in crime prediction based on a single piece of information, such as the colour of someone's trousers (Wang et al., 2005) that could lead to identifying a person’s ethnicity. These developments have increased doubts about the use of FRTs, which are supposed to ensure public secu-

6. Establishing a legal basis for data processing based on consent in AI technologies is problematic and data controllers usually present unreal (or illegal) consent practices. See, Gültekin-Várkonyi, 2019.

rity, but not a wide range of surveillance.

Function creep is usually sought to be legalised by obtaining consent from individuals. This approach, combined with illegal consent practices, could lead to even wider problems, particularly if surveillance is targeted at specific groups. For example, a school in Sweden conducted a trial of FRT to monitor students' attendance. However, this practice was deemed unlawful by the Swedish DPA as the data was processed without explicit consent. Two high schools in France tested a FRT to track students' attendance, similar to the Swedish practice, and the implementation was found unlawful by the French DPA as consent was not properly obtained (CAIDP, 2020). Even though consent could help in achieving successful AI for social good (Floridi et al., 2020), people usually do not have the option to opt out of FRT evaluations in public spaces (Ada Lovelace Institute, 2019). In practice, an illusion to individuals is created as consent is the only legal basis for FRTs (Vogiatzoglou and Marquenie, 2022). An example is the FRT-based solution that was initially developed for pandemic-related purposes, and thus obtained consent for that specific objective, later employed for the identification of problem gamblers with the same data counting around 1 million records (Pearson, 2024). Apparently, the purpose which the consent was given is distinct from the initial one. Additionally, in the previous examples, students essentially pay for their (free) education with their biometric data. The reason for the school administration's adoption of this implementation, whether for student surveillance or to aid in their educational progress, may be unclear to parents who were not involved in the decision-making process and did not request it. As such, they have raised concerns, and here the consent has at LEAs served to raise awareness among parents and correct the improper implementation.

4.3 Risk three: The data accuracy challenge

It is crucial to remember that the life-source of an AI system is data. In order for an AI system to generate accurate and unbiased outputs, Article 5(d) of the GDPR suggests that the data processed during the life cycle of an AI system must be accurate and up-to-date. In practice, this principle could help prevent individuals from having wrong accusations based on inaccurate data in police databases which may even result in imprisonment (Hill, 2020). Similarly, accurate data could prevent individuals from being repeatedly stopped and questioned by the police (*Dimitrov-Kazakov v. Bulgaria* 2011). These realities raise concerns about the reliability of the systems and whether they can ensure public security and justice. To mitigate the risk, one solution is to continuously update police databases with data from the operational field of FRT and improve the accuracy of the algorithm (Bergman et al.,

2023). However, this potentially would reinforce surveillance in public (Raposo, 2022). Another solution could be referring to an aggregated database to update the system. This database could be open source, allowing for testable accuracy levels (Delikat, p. 61). However, in reality, providers may prefer to use their own closed database, where accuracy levels cannot be directly tested (Fábián & Gulyás 2021). For instance, the reliability of the system might be compromised if the database includes fake images that do not represent real individuals. It is important that both the LEA and the public can question the source of the data. Technical standards (ASTM, 2023) could help when training the algorithm for FRTs, considering various factors that can influence accuracy, such as hardware specifications, image angles, and data preparation processes. However, these details are often not transparently communicated to the public.

In legal documents and technical contexts, it is important to distinguish between two types of accuracy. The GDPR approaches the principle of data accuracy as the requirement for data to be correct, up-to-date, and rectifiable. In contrast, accuracy in AI terminology refers to the level of accuracy of the output generated by the algorithm and is mathematically or statistically presented. The GDPR refers not only to the accuracy of first-hand personal data but also to indirectly processed personal data that can identify individuals, such as rankings (Hacker et al., 2023). FRTs' rankings should also be considered as personal data and carry specific risks related to the processing of personal data. Therefore, evaluations from FRTs are also considered personal data, as they probabilistically rank people according to their risk score. As will be demonstrated later, the AIA effectively bridges the gap between data accuracy and system accuracy, although challenges still persist.

4.4 Risk four: Administrative challenges

In the public sector, software and hardware products are typically outsourced to the private IT sector, which offers a wide range of high-quality systems that a LEA cannot develop in-house. According to the USGAO report on the algorithms used in federal law enforcement (2020), half of the AI-based systems used by US federal LEAs are outsourced to private companies. The report highlights that authorities may lack technical knowledge of the FRTs they are using, which could hinder their ability to anticipate and assess the human rights risks posed by these systems. Additionally, a separate study found that most Americans would welcome FRTs if police were properly trained in their use (Raine et al., 2022). However, in practice, the police tend to prioritise the effectiveness of the software over its development and operation (Urqhuart, p.15). The LEAs should ensure that they clearly communicate their roles and duties in operating FRTs to the public, and participate in possible

technical settings of the system (see the system accuracy title later for an in-depth analysis).

Identifying clear roles in the operation of FRT is a tool to enhance transparency and accountability. Once faced with an algorithmic evaluation, people often are confused on whom to turn to ask for explanations specific to their cases. The GDPR identifies three actors involved with data handling that are data controllers, data processors and joint controllers. Their responsibility (either sole, joint, or shared) level is not equally weighted between these categories since they take different roles. It is common practice in the IT sector that the data passes back and forth between many data controllers and processors, which may make it difficult to identify the real responsibility (Gültekin-Várkonyi, 2020, p. 198). Even from the legal perspective, distinguishing and identifying these roles clearly is uncertain, which reduces the impact of the fines to be imposed (Mahieu et al., 2019). Moreover, controlling processed data proves difficult as it neither falls under public domain nor is readily accessible to public institutions. The commercial development of FRTs by private companies further exacerbates the situation, as public trust in these entities tends to be lower than in public actors (Ada Lovelace Institute et al., 2021). The use of ChatGPT increases among LEAs, they may sometimes unknowingly transmit personal data to other partners of OpenAI, potentially eroding public trust if such usage remains undisclosed. Hence, the importance of defining clear roles cannot be overstated, as the deployment of FRT systems by unprepared law enforcement personnel risks eroding public trust without proper understanding and oversight.

4.5 Summary

The table below summarises the mentioned risks associated with the use of FRTs processing personal data in public spaces evaluated under the GDPR.

TABLE 1: Risks associated with FRTs under the GDPR

RISK	DESCRIPTION	EXPLANATION
Data minimisation	Operation of FRT in public spaces often causes mass data collection, leading to constant surveillance that undermines autonomy and freedom.	Surveillance technologies intended to protect public security violate the principle of data minimisation leaving individuals and groups unable to exercise their rights ensured in the GDPR.
Purpose limitation	AI systems offer distinctive opportunities for data collected for one purpose to be used for another, potentially violating lawful data processing and transparency principles.	Operating FRTs challenge the protection of public interest by misusing data beyond its original intent, which is public security, undermining public trust and personal freedoms.
Data accuracy	Inaccurate data in FRT systems can lead to wrongful accusations, directly harming	Inaccurate data compromises both public security and public interest by leading to wrongful actions

RISK	DESCRIPTION	EXPLANATION
	individuals' rights and freedoms	and undermining the reliability of FRTs.
Administrative challenges	Outsourcing AI systems to private companies creates a knowledge gap in LEAs, hindering their ability to manage and anticipate data governance risks associated with FRTs.	Challenges in practical and technical management of FRTs reduce transparency and accountability, thereby diminishing public interest in surveillance measures.

The first risk involves violating the data minimisation rule, which can occur both technically and practically. This violation can lead to excessive surveillance and a loss of individual autonomy referring to having legal consequences. The second risk, function creep, arises from the technical and practical misuse of data for purposes beyond its original intent, which undermines legal rules relevant to transparency and legitimate data processing. The third risk addresses data accuracy issues that are technical and legal, which can lead to wrongful accusations and diminish the reliability of AI systems. The fourth risk focuses on administrative challenges that stem from practical and legal uncertainties, particularly the outsourcing of AI systems, which hampers effective oversight and accountability. Together, these risks regarding processing personal data in FRTs illustrate how surveillance technologies, while intended to enhance public security, can often compromise public interest by violating the right to data protection.

5. Evaluation of the four risks under the AIA

This section analyses the risks introduced by FRTs in law enforcement, focusing on the viewpoint of the AIA and aligning with the scrutiny applied in the GDPR analysis. The AIA classifies AI systems into four risk levels: those with unacceptable risk, high risks that are acceptable under certain regulatory conditions, limited risk, and minimal risk. FRTs that are classified as unacceptable risk should be banned and only allowed in limited, clear, and strict exceptional cases. The AIA establishes general principles aimed at upholding fundamental rights by LEAs and establishing minimum standards for AI systems, but these principles may lack the requisite specificity for FRTs in certain aspects, potentially undermining its main purpose for operation.

5.1 Risk one: Violation of general principles-definitional challenges

The AIA adds further complexities to those mentioned in the GDPR section when interpreting rules and principles. The definitional issues in the Act make it even more challenging to demonstrate transparency of the FRT to the public, thereby reinforcing existing distrust. The very first issue relates to the definition of FRT

from both a legal and technical perspective. Finklea et al. (2020) states that FRT, which may seem like a simple term, can have different technical and legal meanings, and that (like most of the technological terms) there is no clear definition of this technology. The term as it appears in the AIA still does not fully encompass all possible types of AI and remains narrowly defined. For instance, the definition of GPT which could also process biometric data now remains overly inclusive in the Act, attempting to simplify the technology underestimating its technical capabilities (Hacker et al. 2023). This allows providers to interpret the law and ethical standards in a personalised manner, which may differ from the intended meaning (Hacker et al. 2023).

A significant definitional shortcoming in the AIA pertains to the definition of biometric data. The AIA references the GDPR and the LED for defining biometric data, which has a special relation to facial recognition only under French data protection law (Christakis et al., 2022a). This term requires a more detailed evaluation, particularly concerning its application in FRTs used in public spaces for security purposes, and must be clearly explained to the public. Further, the AIA introduces several terms in Article 3, including "biometric identification" (para. 35), "biometric verification" (para. 36), "biometric categorisation system" (para. 40), "remote biometric identification system" (para. 41), "'real-time' remote biometric identification" (para. 42), and "post-remote biometric identification system" (para. 43). These terms may overlap or lack clarity from both practical and technical perspectives, creating a "terms salad with no taste", which only complicates understanding for both deployers and providers. This terminological plurality can impair the public's comprehension of how these technologies function. Moreover, law enforcement agencies (LEAs) often withhold detailed information about the tools they use, citing security reasons. This tendency towards secrecy exacerbates the problem of asymmetric information, where LEAs possess more knowledge than the public. Such an imbalance can result in the deployment of these technologies without adequate public scrutiny, justified under the pretext of security threats (Hacker, 2018, p. 90). Consequently, the actual impact of FRT on public security remains unclear, potentially eroding public trust in these technologies.

The final challenge to be presented here is relevant to the identification of the law applicable to FRTs. Already, there is no legislation clearly limiting the use of technologies by LEAs (Christakis et al., 2021). Existing legislation governing technology use by LEAs is either lacking or opaque, hindering individuals' ability to obtain information and assert their rights (Sherwin et al., 2019; Li, 2019) and weakening their position under power. The challenge of categorising technologies under ap-

propriate legislation is evident, as various AI tools used by law enforcement fall under different laws, lacking specificity to address key issues (Karsai, 2020). Applicable ones allows MS to set rules on biometric data processing, leading to varied interpretations and applications across the EU, weakening the position of the public authorities in defending public interest. Assessing the use of GPT tools by LEA under the GDPR could typically result in a blanket ban due to their capabilities for real-time voice and image analysis, which involve processing biometric data without public awareness. For instance, the Italian DPA temporarily banned ChatGPT for these reasons (Helleputte et al., 2024), although its use remains permitted. On the other hand, the Austrian data protection authority's leniency towards Clearview AI exemplifies divergent regulatory approaches (TIPIK Legal, 2021). This regulatory and definitional ambiguity underscores the need for a clear and uniform approach in application to protect public interest and individual rights.

5.2 Risk two: The challenge of limiting the purposes

The AIA introduces the term intended purpose (Article 3(12)) to align closely with the GDPR, emphasising that AI systems are designed for specific purposes as defined by the provider. Any deviation from this intended purpose is considered misuse. However, if the primary purpose is not clearly adhered to by the deployer, public security could be compromised by the reuse of data – often legally permitted but not always aligned with the intended purpose. For example, in Hungary, facial image systems are primarily used for identification purposes and are regulated in detail (Gárdonyi, 2020). However, the use of facial image data by legally authorised LEAs is complicated by the fact that the law itself (for example, Article 6 of Act CLXXXVIII, 2015) identifies a non-exhaustive list of areas in which FRTs can operate, albeit under certain conditions (Act CLXXXVIII, 2015, p.27). Such reuse, although not technically misuse, may still challenge public security interests if the AI system's intended purpose evolves during use.

The AIA explicitly prohibits real-time remote biometric identification systems, with some exceptions (Article 5(1)(h)). In the parliamentary draft of the AIA (EP, 14 June 2023, T9-0236/2023), the EP advocated for extending this prohibition to include post-remote identification systems. The proposed amendment (nr. 227) in Article 5(1), with the introduction of a new point (d), suggested a ban on the use of post-remote identification systems by LEAs in publicly accessible areas, except with pre-judicial authorization for targeted searches related to specific serious crimes, as defined in Article 83(1) of the Treaty on the Functioning of the European Union.[7] This amendment would have potentially set a higher barrier for the imple-

mentation of post-biometric identification systems. However, this proposal was not adopted in the final text, which maintained the prohibition specifically for real-time biometric identification systems. Consequently, post-remote identification systems are classified not as prohibited AI systems but as high-risk AI systems, with broader exceptions for their use. Additionally, the proposed amendment initially required pre-judicial authorization, but the final version replaced this with administrative authorization, thereby weakening judicial protection of the public interest before LEAs. This change raises concerns about the potential for governmental authorities to repurpose data in post-remote systems for broader uses, leading to inconsistencies in the application of the AIA and varying levels of protection for European citizens. At the time of writing, a joint paper by Germany, France, and Italy emphasised that the AIA should be applied to avoid stifling innovation rather than imposing sanctions (Reuters, 2023; Gstrein et al., 2024). Although all EU member states eventually agreed on the final text, this joint action indicates that there were divergent interests among the members and EU decision-makers regarding the AIA, which could also manifest in the application of security-related exceptions for public interest.

It should be noted that any method of identification, whether remote or not, post or real-time, could lead to function creep and surveillance as the data is used in the system. When the system is fed back by the data collected either in real time post, “threats are not reduced just because authorities or companies have more time to review footage” (Jakubowska, 2023). For these reasons, the limitation of purpose and clear identification of intended purposes have a crucial impact on constraining the potential extensive surveillance practices of LEAs. According to a study (Delikat, 2021), the specified purposes for using FRTs in EU LEAs are generally broad and vary among them, particularly in the context of surveillance. In addition, LEAs often delegate decisions about the fate of data in the system, such as when to store, delete and update personal data, to providers who may not have a full understanding of the legal requirements compared to the LEAs themselves. This dynamic prompts member states to implement measures that restrict data subjects' right of access, ensuring the efficiency of police work while limiting the fundamental rights (FRA, 2019).

7. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime. Obviously, the scope of the exceptions allowing the operation of post-remote identification systems is already extensive, offering LEAs a broad range of permissible activities under these exceptions

5.3 Risk three: The system accuracy challenge

The AIA smoothly makes the connection between data accuracy and system accuracy in the concept of law enforcement. The AIA's Recital 67 highlights the training data to be high quality to ensure accuracy and avoid individuals in a discriminatory, incorrect, or unfair accusations. To ensure the success of a system that also serves public interest, this link is crucial. Article 15 of the AIA explicitly refers to the importance of accuracy in high-risk AI systems, which is considered one of the most crucial transparency requirements for such systems. To enhance accuracy, the expected level of precision and its metrics should be disclosed to deployers (not individuals or the public directly) as instructions. However, evaluating the performance of a FRT system involves different metrics, each providing a unique perspective on the system's results as it is also the case for the FRT (EDPB, 2022). It is unrealistic to expect that all metrics will be included in a single document and easily understood by all LEAs without further communication. This raises several questions.

The initial question that arises is: who determines the planned and tested accuracy level in FRTs. Article 13(3)(2)(ii) AIA states that the accuracy level must be designed by the provider to complement transparency enabling deployers to (only) interpret outputs, without referring clearly to the possibility of the deployer to give any feedback on the planned or enabled accuracy level. It is clear that the provider alone decides on the relevant accuracy of the system during the system design phase. During the implementation of FRTs, there is a risk that the focus might shift solely to system performance metrics, potentially prioritising system performance over public interest considerations. For example, the Metropolitan Police discovered that over 98% of matches in their live biometric data processing during implementation were all in false positives (Big Brother Watch, 2018, p. 25). Different accuracy settings are required for FRTs used for border checks compared to criminal matches, as both applications directly affect fundamental rights. Even within the same context, achieving an acceptable level of accuracy demands a careful and detailed analysis. Distinguishing between classifying someone with 90% confidence as a potential criminal versus 60% confidence is crucial, as the difference significantly impacts an individual's rights. It is evident that there are various approaches to determining the appropriate accuracy levels. The prospect of establishing a unified methodology at the EU level appears, given that the AIA involves the Commission, in collaboration with relevant stakeholders, in addressing the technical aspects of methodologies for measuring suitable accuracy levels in Article 15(2) AIA. Recital 74 of the AIA further specifies the Commission's role in this task, drawing parallels to its involvement in Directive 2014/31/EU on non-auto-

matic weighing instruments and Directive 2014/32/EU on measuring instruments. This points to a probability for the EU to take regulatory or non-regulatory actions to ensure AI accuracy in alignment with broader legal metrology principles.

This involvement raises two key questions. First, how can methodologies for general accuracy measures for a specific technology like FRT and its specific law enforcement applications be identified? If specificity is not sought, then why are the accuracy rules, including quality management rules specified in Article 17 of the AIA, not sufficient? The accuracy rules and the quality management system already give guidance on how the accuracy levels should be aligned with general principles. General methodologies for identifying accuracy levels in a specific technology may not work due to several factors. For instance, from a technical standpoint, face recognition is less accurate than other biometric data, such as fingerprinting (Garvie et al., 2016). Additionally, the potential for inaccuracy in these learning systems is high, as accuracy may change over time with new data. Consequently, periodic revisions on the specific accuracy levels, together with their methodologies, are necessary to ensure the system's reliability. The AIA lacks flexibility and clarity in this regard. The interpretation of relevant articles (Article 15 (2) AIA) should have indicated that accuracy levels are not fixed measurements and should be adjustable based on usage scenarios. Since an FRT cannot be developed solely for one purpose (see “Purpose limitation” section), its accuracy level cannot be singular.

Second, when and how will the Commission, as a political entity, reach a consensus on methodologies for accuracy measurement tools for AI systems used by member states' LEAs? Most parts of the Act will be effective from August 2026, less than two years away, and discussions on sensitive topics like measurement methodologies for high-risk AI systems used for public security have not yet taken place. It will be interesting to observe LEAs' involvement in these discussions, representing their national interests, and whether they can find common ground beyond the general agreements already established.

The ideal solution could have been referred to a more local level, without involving the political bodies in the process. For example, the rules could guide the provider to provide the deployer with detailed explanations of the intended levels of accuracy. Feedback from the provider could be required, which would then increase the transparency of the system (Hacker & Passoth, 2022). In this process, the provider should be aware of the modelling steps needed to mitigate any accuracy risks arising from incorrect use cases. This is because a technology designed for verification might not be effective for searching a criminal database. Further, to

avoid malfunctioning and erroneous outputs, it is essential to use not only data but also highly representative data. As Fontes et al. (2022) explained in their analysis of a privacy-focused Corona app, which dropped representativeness by not collecting sensitive information, highly representative data must be fed to the systems to avoid incorrect outputs. LEAs, who are likely well aware of the groups that might be underrepresented in FRTs, could provide relevant instructions to the providers. LEAs should guide the provider to understand each specific use case and the acceptable accuracy levels from both technical and legal perspectives. This approach enables the provider to gain an understanding of the legal and contextual background of the FRT they develop in a timely manner, rather than at a later stage. Furthermore, it allows the LEAs to communicate this understanding to the public. If the terminology used in technical documents could be translated into accessible language, it is probable that the public would provide feedback on such complex procedures if a feedback system were to be established. By collaborating with the public on such sensitive matters, it may be possible to diminish scepticism towards the systems (and their accuracy) (Urquhart & Melinda, 2021, p. 5), thereby fostering the legitimacy of their use.

5.4 Risk four: Administrative challenges

How difficult is it for individuals to identify a responsible person or persons behind FRTs operated in public spaces? Answering this question, similar to the discussion presented under the GDPR, is not an easy task for the public, and one of the reasons for such difficulty is the administrative relationship between the deployers and the providers. Private entities often exploit legal loopholes to avoid direct responsibility while still maximising profits.[8] This does not imply that they are any less responsible than LEAs, both to LEAs and to the public, when their system is being used. FRT deployers should be able to assign the sole or partial responsibility to the providers, e.g. in case of systemic failure or in extensive data collection measures. The AIA repeats the complexity to administer the issue as per discussion of the same topic under the GDPR. According to Article 3 (46) of the AIA, law enforcement refers to "activities carried out by law enforcement authorities or on their behalf" for several purposes, such as the prevention of threats to public security. Based on this definition, private entities and even individuals could also act on behalf of law enforcement.

8. See, for example, Google's explanation of why FRTs developed by Google are good, referring to the exception in Article 5(d)(i) for the possible use of remote biometric identification systems to search for missing children: "it can also be used for tremendous social good; there are nonprofits using face recognition to fight against the trafficking of minors" (Google AI, n.d.).

This arrangement often lacks clarity regarding the relationship between these external entities and LEAs, leaving the public uncertain about who should be held accountable for any misuse or errors, whether it be the LEA, the third-party operator, or both. It complicates for the LEA the issue of responsibility not only in cases of system failure (Moss & Metcalf, 2019), but raises uncertainties to the public about where to direct complaints or seek redress for potential data misuse, the LEA or the private entity? Moreover, the involvement of third-party operators, particularly those across different jurisdictions (such as the Clearview AI operated by a US-based company), may cause legal complexities. Varying standards for data protection, accuracy, and liability across jurisdictions can lead to difficulties in coordination and may result in legal conflicts or challenges in enforcing EU regulations in a wider sense.

5.5 Summary

The table below is to summarise the mentioned risks associated with the use of FRTs in public spaces evaluated under the AIA.

TABLE 2: Risks associated with FRTs under the AIA

RISK	DEFINITION	EXPLANATION
Definitional challenges	The AIA introduces complex and unclear definitions for terms like biometric data and related technologies. It further refers to other laws for defining biometric data, but these definitions are not always clear or consistent.	The lack of clear definitions makes it difficult for the public to understand FRTs and leaves LEAs to rely on their own understanding of the term, complicating public scrutiny and potentially allowing misuse by LEAs.
Purpose limitation	The AIA defines "intended purpose" but does not address potential re-use or function creep of FRTs by LEAs.	Broad and vague definitions of purpose can lead to extensive surveillance, potentially exceeding the original scope, compromising public interest.
System accuracy	The AIA emphasises system accuracy but leaves ambiguity regarding how accuracy levels should be determined and adjusted.	Unclear guidelines and over regulation on accuracy metrics can lead to improper use of FRTs, causing incorrect results and potential harm to individuals if the systems perform inadequately.
Administrative challenges	The AIA further allows delegation of law enforcement activities to third-party operators, complicating responsibility.	Involvement of private entities can create legal ambiguities and make it unclear who is accountable in cases of system failure or misuse.

The first risk involves definitional issues which stems from legal challenges that create confusion about the technology's scope and application, complicating effective regulation and public understanding. The second risk addresses the challenge of limiting FRT purposes which occurs from legal, technical, and practical reasons, where unclear or evolving uses can lead to misuse and excessive surveillance, potentially compromising public security. The third risk pertains to system accuracy,

both a legal and a technical challenge, where inconsistent or inadequate accuracy standards can result in unreliable technology, impacting its effectiveness in ensuring security. Lastly, as a legal and practical challenge, administrative challenges arise from the complexities in assigning responsibility and ensuring accountability between LEAs and third-party providers, complicating oversight and enforcement. These risks collectively highlight how the deployment and regulation of FRTs can affect public security and interests, underscoring the need for clear, consistent guidelines and robust management to prevent misuse and ensure effective oversight.

6. A suggested solution: Enhancing the role of data protection impact assessment for a more legitimate FRT

In order to serve the public interest in a genuine manner, LEAs must demonstrate that FRTs benefit not only their operational needs but also the public good. A bottom-up approach, whereby LEAs gain public trust by first addressing individual privacy and data protection concerns, may prove more effective than a top-down legislative approach. A strategy based on incremental steps could help to avoid a total breakdown. One starting point with this aim is, as this article proposes, to enhance the Data Protection Impact Assessment (DPIA) and integrate it to the existing risk management system of the AIA, even if it is not a comprehensive solution alone.

The AIA introduces minimum standards to ensure that fundamental rights are respected throughout the lifecycle of AI systems. To ensure this, it introduces obligations for those involved in the development, marketing, and operation of the system. These obligations have much in common with the GDPR. For example, high-risk AI systems must undergo a fundamental rights impact assessment (FRIA) as indicated in the Article 27 of the AIA before they are placed on the market. This assessment is made by the deployer to measure in what ways a certain AI system would put fundamental rights at risk, from the aspects of defining how and when the system will be used, who it might affect, and how humans will oversee the system. In the end, the deployers also should present how these risks would be mitigated. This is similar to the DPIA required by Article 35 of the GDPR. The law only requires the FRIA for aspects not covered by the DPIA, which creates a link between the two and they complement each other.

It should be emphasised that the DPIA focuses on assessing risks related to data processing but does not cover potential issues such as government surveillance,

bias, or accuracy testing. The DPIA is conducted by data controllers to meet accountability and transparency requirements primarily for public authorities, not directly for the public. To address the broader risks highlighted in this article, it is proposed to expand the scope of the DPIA by incorporating new assessment topics, rather than creating entirely new frameworks. This approach allows for specific applications, such as in healthcare, without redundancy (Gültekin-Várkonyi & Gradišek, 2020). In contrast, the FRIA is carried out by the deployers of AI systems, often without the involvement of providers who could offer essential technical guidance. For instance, evaluating the risks posed by technologies like FRTs, especially those affecting specific groups (as indicated in Article 27(1)(d)), would benefit from collaboration with the original system designers. However, the implementation of these assessments might be less problematic under the AIA, which introduces a comprehensive risk management system. This system is designed to be continuous and iterative, covering the entire lifecycle of the AI system. It integrates the principles of both DPIA and FRIA, ensuring that risks to fundamental rights and data protection are continuously identified, evaluated, and mitigated. The goal is to ensure that AI systems are developed and deployed in ways that protect individual rights and serve the public interest.

At this point, DPIAs could be imagined as an integrated part of a broader risk management system, but it still should be considered as a separate and specific mechanism for evaluation of the personal data to be processed. For LEAs, DPIAs offer a unique perspective that allows them to fully assess risks through the lens of public perception specific to their personal data protection, thereby facilitating more informed decision-making processes. Including public engagement in DPIAs could promote transparency and increase confidence in the intended function of LEAs, which is to provide security rather than facilitate widespread surveillance. However, the existing literature and practices do not refer to a specific DPIA for FRTs at LEAs during the course of my research for this article. The only literature found during the preparation of this article was by Castellucia and Le Mateyer (2020), who proposed a DPIA specifically designed for FRTs. It is important to note that this report was published before the AIA and therefore does not take it into account.

Existing literature on DPIA strongly emphasises the need for public participation in impact assessments (Bondi et al., 2021). Public consultation is often overlooked in the formulation of DPIAs, and existing practices often fail to inform the public effectively, relying solely on ex-post public awareness initiatives, such as publishing information on police websites or social media accounts, as exemplified by the

2020 Bridges vs CCSWP case. If an assessment of data processing is to be made, it must be made before data is processed in an AI system, and should include public access and public consultation before data is processed (Moss et al., 2021). If the various interests of the public (data protection interests, as specifically focused on this article) are not represented during the development of the system and if they are not given the opportunity to contribute, this can lead to an incomplete system design, which can later cause the project to fail (Züger & Asghari, 2023, p. 820). This failure would affect both providers and LEAs, not only from a legal point of view, but also from a technical and practical point of view. Sloane et al. (2022) suggest several ways in which stakeholders could participate in the DPIA. For example, FRT providers could consider a consultative approach to participation in conjunction with the LEAs, as mentioned in the system accuracy section of this article.

In light of the findings from the literature presented, it is paramount to ensure the public's active involvement and representation in the design process of FRTs. Individuals and the public could be involved in DPIAs in many ways. For example, providers and deployers could consider involving members of the public as external reviewers of the DPIA. This way, public feedback should be taken into account in the further decision-making process. To ensure impartiality, but also to make participation attractive, they could offer benefits to participants, such as a gift (e.g. a cinema ticket), which would not bias their feedback towards the interests of the deployer or the provider. In addition, academics and non-profit organisations could be involved in the preparation of the DPIA. Based on all of these analyses, I suggest in the table below that several questions be considered to be raised during the DPIA, which represent sub-assessment points for the already existing requirements specified in both pieces of legislation.

TABLE 3: Specific impact assessment questions for FRT in law enforcement

	PURPOSE LIMITATION	ADMINISTRATIVE	DATA ACCURACY	SYSTEM ACCURACY
TECHNICAL	Does the FRT work for multiple purposes (e.g. emotion recognition) or only for one or more of the following: identification, authorization, surveillance.	Is the FRT integrated with another system or does it operate as a stand-alone system? If integrated, how are risks mitigated across the multiple systems?	1. What technical standards will be used to capture the biometric data? What steps are taken if the enrolled data is not qualified according to the standards? 2. Which source library does the biometric belong to? Has the source library been tested for bias, discrimination, accuracy, and leakage? 3. How often is the data	1. What steps are taken to ensure that the FRT does not produce inaccurate results? Is the accuracy of the FRT checked regularly? 2. Is the level of accuracy standard for each assessment or is there a dynamic level of accuracy for different assessment cases?

	PURPOSE LIMITATION	ADMINISTRATIVE	DATA ACCURACY	SYSTEM ACCURACY
			updated? How often is unnecessary and/or inaccurate data discarded?	3. Why and how is this level of accuracy chosen? Is it reviewed from time to time? Who decides on the accuracy level and on what basis?
PRACTICAL	Where will the FRT operate and, if possible, at what time of day? What will be the main purpose of this operation?	1. Is training planned for the staff who will be using the FRT? If so, what are the main aspects of the training? (system use, legal assessment, both?) 2. Who are the actors that can process data on behalf of the LEA? 3. Is there any public feedback involved in the development of the FRT?	1. Is the output data fed back into the system? If so, is the assessment repeated? 2. How could people access and manage their data? How could they request the rectification of their data?	How could people contest the outputs that they think are wrong?
LEGAL	1.Is the FRT being developed initially for law enforcement purposes? If not, how will the system be integrated for law enforcement use? 2. Is the data in the FRT processed real-time, post or both? How does the chosen method help to achieve the original purpose of the system?	Are there any other authorities which may have access to the FRT or have a request for access to the FRT? If so, in what specific cases could they do so?	Will the biometric data in the FRT be combined with any other data (e.g. health data, financial data)?	

The table presents the points discussed in the previous sections under the four risk headings. As a reminder, each title has addressed the risks from either a technical, legal, or practical perspective. Therefore, the proposed questions to extend the scope of the DPIA to specifically focus on the use of FRT in LEAs also contain practical, legal and technical assessment points that aim to guide these actors to operate FRT in a more data protection rights friendly way. A note must be made here about the language to be used in the DPIAs, especially since they are supposed to be made publicly available. There is a difference between the purpose of the FRT (authentication, identification, or surveillance) and the information on these purposes to be provided to the public (Matulionyte, 2024). As DPIA is also one of the transparency tools and, since it contains many technical and legal assessments, one DPIA format designed in a general language might not be enough. The information to be delivered in the DPIA should be selected based on the public knowledge of the FRT, taking into account the potential for there to be individuals with limited expertise in FRTs and another group of the public who are experts on the topic. Finally, ensuring the delivery of communication in languages other than the

dominant language is crucial for fostering inclusiveness.

This table is not final and is indeed open to further improvement. The questions in the relevant areas aim to fill current gaps that may arise in practice and can be further improved and are therefore complementary to those that already exist in the legal requirements. In an era of limitless technology, aligning legal rules with practical guidance may help strengthen the protection of human rights in the face of new and relatively risky technology.

7. Conclusion

FRT offers LEAs significant opportunities in public security, with applications in authentication, identification, and profiling. As these technologies heavily rely on biometric data, their use by law enforcement is scrutinised only under legislation, mainly the GDPR and AIA, emphasising the need for more practices to comply with more public interest centric applications.

The risks posed by FRTs in law enforcement include challenges with data minimisation, function creep, accuracy, and administrative complexities. Data minimisation concerns arise from the constant collection of biometric data, potentially infringing on privacy and anonymity. Function creep occurs when algorithms exceed their intended purposes, leading to potential misuse by both private entities and LEAs. Accuracy issues under the GDPR and AIA pose difficulties in correcting and updating data, while the AIA's allocation of responsibility adds to these challenges. Administrative complications stem from outsourcing FRTs, creating a complex network of accountability that could undermine public trust.

To mitigate these risks and enhance public confidence, LEAs must clearly demonstrate that the tool is planned to be used for its sole purpose. Extending the scope of the DPIA as an integral part of FRIA to specifically address FRT in law enforcement could improve transparency and effectiveness. Ultimately, the development and use of FRTs should be guided by public opinion to ensure they meet both security needs and individual privacy concerns.

NOTE

This article is an updated and extended version of its unpublished version drafted in Turkish for the book by Karsai et al. (2022).

References

Ada Lovelace Institute. (2019). *Beyond face value: Public attitudes to facial recognition technology* [Report]. https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

Ada Lovelace Institute, AI Now Institute, & Open Government Partnership. (2021). *Algorithmic accountability for the public sector* [Report]. https://www.opengovpartnership.org/documents/algorithmic-accountability-public-sector/

Akbari, A. (2024). Facial recognition technologies 101: Technical insights. In R. Matulionyte & M. Zalnieriute (Eds.), *The Cambridge handbook of facial recognition in the modern state* (pp. 29–43). Cambridge University Press. https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technologies-101/8B3039F97B11F43B78E52BBEB73E8479

American Society for Testing and Materials. (2023). *Standard guide for capturing facial images for use with facial recognition systems* (Volume: 14.02 Nos. E3115-17). ASTM International. https://doi.org/10.1520/E3115-17

Amnesty International. (2023, December 9). *EU: Bloc's decision to not ban public mass surveillance in AI Act sets a devastating global precedent*. https://www.amnesty.org/en/latest/news/2023/12/eu-blocs-decision-to-not-ban-public-mass-surveillance-in-ai-act-sets-a-devastating-global-precedent/

Bergman, A. S., Hendricks, L. A., Rauh, M., Wu, B., Agnew, W., Kunesch, M., Duan, I., Gabriel, I., & Isaac, W. (2023). Representation in AI evaluations. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 519–533. https://doi.org/10.1145/3593013.3594019

Big Brother Watch. (2018). *Face off: The lawless growth of facial recognition in UK policing* [Report]. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Björklund, F. (2021). Trust and surveillance: An odd couple or a perfect pair? In L. A. Viola & P. Laidler (Eds.), *Trust and transparency in an age of surveillance* (pp. 183–200). Routledge. https://doi.org/10.4324/9781003120827

Bondi, E., Xu, L., Acosta-Navas, D., & Killian, J. A. (2021). Envisioning communities: A participatory approach towards AI for social good. *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 425–436. https://doi.org/10.1145/3461702.3462612

Borak, M. (2024, May 8). Police in Germany using live facial recognition. *Biometric Update*. https://www.biometricupdate.com/202405/police-in-germany-using-live-facial-recognition

Bowling, B., & Iyer, S. (2019). Automated policing: The case of body-worn video. *International Journal of Law in Context*, *15*(2), 140–161. https://doi.org/10.1017/S1744552319000089

Bragias, A., Hine, K., & Fleet, R. (2021). 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research*, *22*(6), 1637–1654. https://doi.org/10.1080/15614263.2021.1942873

Bridges v CCSWP (Approved judgment No. 2020 EWCA Civ 1058). (2020). The Court of Appeal. https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf

Bridges v CCSWP (High Court judgment No. 2019 EWHC 2341). (2019). The High Court of Justice. https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

Castelluccia, C., & Le Métayer, D. (2020). *Impact analysis of facial recognition: Towards a rigorous methodology* (No. hal-02480647). HAL open science. https://hal.archives-ouvertes.fr/hal-02480647/document

Center for AI and Digital Policy. (2020). *Report on facial recognition summarizing artificial intelligence and democratic values: Artificial intelligence social contract index 2020* (Report No. AISCI-2020). https://s899a9742c3d83292.jimcontent.com/download/version/1614781162/module/8293511263/name/CAIDP-AISCI-2020-FacialRecognition-%28Feb2021%29.pdf

Christakis, T., Bannelier, K., Castelluccia, C., & Le Métayer, D. (2022a). *A quest for clarity: Unpicking the "catch-all" term* (Report No. Part 1; Mapping the Use of Facial Recognition in Public Spaces in Europe). Multidisciplinary Institute in Artificial intelligence. https://ai-regulation.com/facial-recognition-in-europe-part-1/

Christakis, T., Bannelier, K., Castelluccia, C., & Le Métayer, D. (2022b). *Classification* (Report No. Part 2; Mapping the Use of Facial Recognition in Public Spaces in Europe). Multidisciplinary Institute in Artificial intelligence. https://ai-regulation.com/wp-content/uploads/2022/05/Facial-Recognition-in-Europe-Part2.-Classification.pdf

Christakis, T., Becuywe, M., & AI-Regulation Team. (2021). *Facial recognition in the draft European AI regulation: Final report on the high-level workshop held on April 26, 2021* [Report]. AI-Regulation.com. https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/

Chui, M., Harryson, M., Manyika, J., Roberts, R., Chung, R., Nel, P., & van Heteren, A. (2018). *Applying artificial intelligence for social good* [Discussion paper]. McKinsey Global Institute. https://www.mckinsey.com/featured-insights/artificial-intelligence/applying-artificial-intelligence-for-social-good

Clayton, J., & Derico, B. (2023, March 28). Clearview AI used nearly 1m times by US police, it tells the BBC. *BBC News*. https://www.bbc.com/news/technology-65057011

Consultative Committee of the Convention 108. (2019). *Guidelines on artificial intelligence and data protection* (Guideline No. T-PD(2019)01). Council of Europe, Directorate General of Human Rights and Rule of Law. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Consultative Committee of the Convention 108. (2021). *Guidelines on facial recognition* (Guideline No. T-PD(2020)03rev4). Council of Europe, Directorate General of Human Rights and Rule of Law. https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html

Council of the European Union. (2023). *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world* [Press release]. https://www.consilium.europa.eu/en/press/press-releAes/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

Cowls, J. (2021). 'AI for social good': Whose good and who's food? Introduction to the special issue on artificial intelligence for social good. *Philosophy & Technology*, *34*(Suppl 1), 1–5. https://doi.org/10.1007/s13347-021-00466-3

De Cremer, D. (2020, September 3). What does building a fair AI really entail? *Harvard Business Review*. https://hbr.org/2020/09/what-does-building-a-fair-ai-really-entail

Degli-Esposti, S., & Arroyo, D. (2021). Trustworthy humans and machines: Vulnerable trustors and

the need for trustee competence, integrity, and benevolence in digital systems. In L. A. Viola & P. Laidler (Eds.), *Trust and transparency in an age of surveillance* (pp. 201–220). Routledge. https://doi.org/10.4324/9781003120827

Delikat, R. (2021). *The regulatory gap between the law and the use of real-time Facial Recognition Technology by police in the European Union* [Master's thesis, Tilburg University]. https://arno.uvt.nl/show.cgi?fid=155401

Dimitrov-Kazakov v. Bulgaria (Execution of Judgment No. Application No. 11379/03). (2018). European Court of Human Rights. https://hudoc.echr.coe.int/eng?i=001-103258

European Commission. (2024). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (No. COM/2021/206). European Parliament and Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

European Data Protection Board. (2020). *Guidelines 3/2019 on processing of personal data through video devices* (Version 2.0 No. Guideline). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

European Data Protection Board. (2021). *Swedish DPA: Police unlawfully used facial recognition app* [Press release]. https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en#:~:text=IMY%20imposes%20an%20administrative%20fine,of%20the%20Criminal%20Data%20Act

European Data Protection Board. (2022). *Facial recognition: Italian SA fines Clearview AI EUR 20 million* [News item]. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

European Data Protection Board. (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* [Version 2.0]. https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

European Data Protection Supervisor. (2021). *Artificial Intelligence Act: A welcomed initiative, but ban on remote biometric identification in public space is necessary* (Press Release No. EDPS/2021/09). https://edps.europa.eu/system/files/2021-04/EDPS-2021-09-Artificial-Intelligence_EN.pdf

European Digital Rights. (2021). *European Commission adoption consultation: Artificial Intelligence Act*. https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf

European Digital Rights. (2023). *EU AI Act: Deal reached, but too soon to celebrate* [Press release]. https://edri.org/our-work/eu-ai-act-deal-reached-but-too-soon-to-celebrate/

European Parliament. (2023). *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

European Union Agency for Fundamental Rights (FRA). (2018). *Handbook on European data protection law: 2018 edition* [Handbook]. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

European Union Agency for Fundamental Rights (FRA). (2019). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement* (FRA Focus) [Report]. https://fra.e

uropa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Europol. (2023). *ChatGPT: The impact of large language models on law tnforcement* (Tech Watch Flash) [Report]. Europol Innovation Lab. https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The

Fábián, I., & Gulyás, G. G. (2021). A comparative study on the privacy risks of face recognition libraries. *Acta Cybernetica*, *25*(2), 233–255. https://doi.org/10.14232/actacyb.289662

Finklea, K., Harris, L. A., Kolker, A. F., & Sargent, J. F., Jr. (2023). *Federal law enforcement use of facial recognition technology* (Report No. R46586). Congressional Research Service. https://sgp.fas.org/crs/misc/R46586.pdf

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy & Technology*, *29*(4), 307–312. https://doi.org/10.1007/s13347-016-0220-8

Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2020). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics*, *26*(3), 1771–1796. https://doi.org/10.1007/s11948-020-00213-5

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: Why we (might) need them and how we want them. *Technology in Society*, *71*. https://doi.org/10.1016/j.techsoc.2022.102137

Gárdonyi, G. (2020). Állóképes arckép azonosítás Magyarországon [Still image face recognition in Hungary]. *Belügyi Szemle*, *68*(3), 22–33. https://doi.org/10.38146/BSZ.SPEC.2020.3.2

Garvie, E., Bedoya, A., & Frankle, J. (2016). *The perpetual line-up: Unregulated police face recognition in America* [Report]. Center on Privacy & Technology at Georgetown Law. https://www.perpetuallineup.org/risk-framework

Gillis, A., Loshin, P., & Cobb, M. (2021, July). Biometrics. *Techtarget*. https://www.techtarget.com/searchsecurity/definition/biometrics

Google A.I. (n.d.). *Our approach to facial recognition*. https://ai.google/responsibility/facial-recognition

Gstrein, O. J., Haleem, N., & Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1790

Gültekin-Várkonyi, G. (2019). Consent mechanism in the life with social robots. *European Review of Public Law*, *31*(1).

Gültekin-Varkonyi, G. (2020). *Application of the General Data Protection Regulation on household social robots* [Doctoral thesis, University of Szeged]. https://doi.org/10.14232/phd.10627

Gültekin-Várkonyi, G., & Gradisek, A. (2020). Data protection impact assessment case study for a research project using artificial intelligence on patient data. *Informatica*, *44*(4). https://doi.org/10.31449/inf.v44i4.3253

Hacker, P. (2018). The ambivalence of algorithms: Gauging the legitimacy of personalized law. In M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), *Personal data in competition, consumer protection and intellectual property law* (Vol. 28, pp. 85–117). Springer. https://doi.org/10.1007/978-3-662-57646-5_5

Hacker, P. (2023). *AI regulation in Europe: From the AI Act to ruture regulatory challenges*. arXiv. https://doi.org/10.48550/arXiv.2310.04072

Hacker, P., Cordes, J., & Rochon, J. (2024). Regulating gatekeeper artificial intelligence and data: Transparency, access and fairness under the Digital Markets Act, the General Data Protection Regulation and beyond. *European Journal of Risk Regulation*, *15*(1), 49–86. https://doi.org/10.1017/err.2023.81

Hacker, P., Engel, A., & Mauer, M. (2023). Regulating ChatGPT and other large generative AI models. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 1112–1123. https://doi.org/10.1145/3593013.3594067

Hacker, P., & Passoth, J.-H. (2022). Varieties of AI explanations under the law. From the GDPR to the AIA, and beyond. In A. Holzinger, R. Goebel, R. Fong, T. Moon, K.-R. Müller, & W. Samek (Eds.), *xxAI - Beyond explainable AI* (Vol. 13200, pp. 343–373). Springer. https://doi.org/10.1007/978-3-031-04083-2_17

Hamann, K., & Smith, R. (2019, May 30). Facial recognition technology: Where will it take us? *Criminal Justice ABA Magazine*, *.19*, 9–13. https://pceinc.org/wp-content/uploads/2019/11/20190528-Facial-Recognition-Article-3.pdf

Hardin, R. (2001). Conceptions and explanations of trust. In K. S. Cook (Ed.), *Trust in society* (pp. 3–39). Russell Sage Foundation. https://www.jstor.org/stable/10.7758/9781610441322.5

Helleputte, C., Belotti, S., & Cieri, F. (2024, April 9). The Italian DPA has its eyes on biometric IDs – Another fight on tech or a win for privacy? *Privacy World*. https://www.privacyworld.blog/2024/04/the-italian-dpa-has-its-eyes-on-biometric-ids-another-fight-on-tech-or-a-win-for-privacy/

Herreros, F. (2023). The state and trust. *Annual Review of Political Science*, *26*, 117–134. https://doi.org/10.1146/annurev-polisci-051921-102842

Hill, K. (2022, August 3). Wrongfully accused by an algorithm. *New York Times*. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Hodge, S. D., Jr. (2020). Big brother is watching: Law enforcement's use of digital technology in the twenty-first century. *University of Cincinnati Law Review*, *89*(1), 30–83. https://scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1374&context=uclr

Hoey, A. (1998). Techno-cops: Information technology and law enforcement. *International Journal of Law and Information Technology*, *6*(1), 69–90. https://doi.org/10.1093/ijlit/6.1.69

Hough, M., Jackson, J., & Bradford, B. (2013). The drivers of police legitimacy: Some European research. *Journal of Policing, Intelligence and Counter Terrorism*, *8*(2), 144–165. https://doi.org/10.1080/18335330.2013.821735

Information Commissioner's Office. (2021). *Information Commissioner's opinion: The use of live facial recognition technology in public place* [Opinion]. https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Jakubowska, E. (2023). *Remote biometric identification: A technical & legal guide* [Guidance]. European Digital Rights. https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/

Jeong, S. (2023, October 10). Assessing algorithms for public good. *The Regulatory Review*. https://www.theregreview.org/2023/10/10/jeong-assessing-algorithms-for-public-good/

Kääriäinen, J. (2008). Why do the Finns trust the police? *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *9*(2), 141–159. https://doi.org/10.1080/14043850802450294

Karsai, K. (2020). Algorithmic decision making and issues of criminal justice – A general approach. In M. C. Dumitru (Ed.), *In honorem Valentin Mirişan* (pp. 146–161). Universul Juridic SRL. http://publicatio.bibl.u-szeged.hu/id/eprint/18429

Karsai, K., Sözüer, A., & Wörner, L. (Eds.). (2022). *Digital criminal justice: A studybook selected topics for learners and researchers*. Onikilevha. https://www.onikilevha.com.tr/yayin/2586/digital-criminal-justice-a-studybook-selected-topics-for-learners-and-researchers

Kindt, E. (2020). A first attempt at regulating biometric data in the European Union. In A. Kak (Ed.), *Regulating biometrics: Global approaches and urgent questions* (pp. 62–69). AI Now Institute. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

Koops, B.-J. (2021). The concept of function creep. *Law, Innovation and Technology*, *13*(1), 29–56. https://doi.org/10.1080/17579961.2021.1898299

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1). https://doi.org/10.1016/j.giq.2022.101761

Li, S. (2019, November 4). Chinese professor files rare lawsuit over use of facial-recognition technology. *The Wall Street Journal*. https://www.wsj.com/articles/chinese-professor-files-rare-lawsuit-over-use-of-facial-recognition-technology-11572884626

Lyon, D. (2002). *Surveillance as social sorting: Privacy, risk and automated discrimination* (1st ed.). Routledge. https://doi.org/10.4324/9780203994887

Lyon, D. (2022). Surveillance. *Internet Policy Review*, *11*(4). https://doi.org/10.14763/2022.4.1673

Mahieu, R., van Hoboken, J., & Asghari, H. (2019). Responsibility for data protection in a networked world: On the question of the dontroller, "effective and complete protection" and its application to data access rights in Europe. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, *10*(1), 84–104. http://nbn-resolving.de/urn:nbn:de:0009-29-48796

Mansfield, T. (2023). *Facial recognition technology in law enforcement: Equitability study, final report* (Final Report No. MS 43). National Physical Laboratory. https://science.police.uk/delivery/resources/operational-testing-of-facial-recognition-technology/

Matulionyte, R. (2024). Increasing transparency around facial recognition technologies in law enforcement: Towards a model framework. *Information & Communications Technology Law*, *33*(1), 66–84. https://doi.org/10.1080/13600834.2023.2249781

Mazzucato, M., Schaake, M., Krier, S., & Entsminger, J. (2022). *Governing artificial intelligence in the public interest* (Working Paper No. IIPP WP 2022/12). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/public-purpose/wp2022-12

Mobilio, G. (2023). Your face is not new to me – Regulating the surveillance power of facial recognition technologies. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1699

Moss, E., & Metcalf, J. (2019, November 14). The ethical dilemma at the heart of big tech companies. *Harvard Business Review*. https://hbr.org/2019/11/the-ethical-dilemma-at-the-heart-of-big-tech-companies

Moss, E., Watkins, E. A., Singh Ranjit, E. M. C., & Metcalf, J. (2021). *Assembling accountability:*

Algorithmic impact assessment for the public interest [Report]. Data & Society. https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/

Moy, L. (2021). Facing injustice: How face recognition technology may increase the incidence of misidentifications and wrongful convictions. *William & Mary Bill of Rights Journal*, *30*, 337–372. https://doi.org/10.2139/ssrn.4101826

Murphy, K. (2013). Policing at the margins: Fostering trust and cooperation among ethnic minority groups. *Journal of Policing, Intelligence and Counter Terrorism*, *8*(2), 184–199. https://doi.org/10.1080/18335330.2013.821733

Nguyen, M.-T., Son, N. H., & Linh, L. T. (2023). Gain more with less: Extracting information from business documents with small data. *Expert Systems with Applications*, *215*. https://doi.org/10.1016/j.eswa.2022.119274

Norris, C. (2002). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), *Surveillance as social sorting* (pp. 249–281). Routledge. https://doi.org/10.4324/9780203994887

Noyb - European Center for Digital Rights. (2023). *Clearview AI data use deemed illegal in Austria, however no fine issued* [News]. https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued

Palmiotto, F. (2024). When is a decision automated? A taxonomy for a fundamental rights analysis. *German Law Journal*, *25*(2), 210–236. https://doi.org/10.1017/glj.2023.112

Palmisano, F., & Sacchi, A. (2024). Trust in public institutions, inequality, and digital interaction: Empirical evidence from European Union countries. *Journal of Macroeconomics*, *79*. https://doi.org/10.1016/j.jmacro.2023.103582

Pearson, J. (2024, May 2). The breach of a face recognition firm reveals a hidden danger of biometrics. *Wired*. https://www.wired.com/story/outabox-facial-recognition-breach

Plangger, K., Marder, B., Montecchi, M., Watson, R., & Pitt, L. (2023). Does (customer data) size matter? Generating valuable customer insights with less customer relationship risk. *Psychology & Marketing*, *40*(10), 2016–2028. https://doi.org/10.1002/mar.21866

Raine, L., Funk, C., Anderson, M., & Tyson, A. (2022). *AI and human enhancement: Americans' openness is tempered by a range of concerns* [Report]. Pew Research Center. https://www.pewresearch.org/internet/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/

Raposo, V. L. (2023). (Do not) remember my face: Uses of facial recognition technology in light of the general data protection regulation. *Information & Communications Technology Law*, *32*(1), 45–63. https://doi.org/10.1080/13600834.2022.2054076

Reuters. (2023, November 20). EU AI Act: Germany, France and Italy reach agreement on the future of AI regulation in Europe. *Euronews*. https://www.euronews.com/next/2023/11/19/eu-ai-act-germany-france-and-italy-reach-agreement-on-the-future-of-ai-regulation-in-europe

Rezende, I. N. (2020). Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, *11*(3), 375–389. https://doi.org/10.1177/2032284420948161

Selwyn, N., Andrejevic, M., O'Neill, C., Gu, X., & Smith, G. (2024). Facial recognition technology: Key issues and emerging concerns. In R. Matulionyte & M. Zalnieriute (Eds.), *The Cambridge handbook of*

facial recognition in the modern state (pp. 11–28). Cambridge University Press. https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technology/20D933F03A88EB412EE6423577FF7F17

Sherwin, E., & Baryshewa, E. (2019, June 11). Russian court rejects facial recognition technology ban. *DW News*. https://www.dw.com/en/russian-court-rejects-call-to-ban-facial-recognition-technology/a-51135814

Shi, Z. R., Wang, C., & Fang, F. (2020). *Artificial intelligence for social good: A survey* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2001.01818

Sloane, M., Moss, E., Awomolo, O., & Forlano, L. (2022). Participation is not a design fix for machine learning. *Proceedings of the 2nd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization*, 1–6. https://doi.org/10.1145/3551624.3555285

Solarova, S., Podroužek, J., Mesarčík, M., Gavornik, A., & Bielikova, M. (2023). Reconsidering the regulation of facial recognition in public spaces. *AI and Ethics*, *3*(2), 625–635. https://doi.org/10.1007/s43681-022-00194-0

TELEFI project. (2021). *Summary report of the project 'Towards the European level exchange of facial images'* (Report No. Version 1.0). https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

TIPIK Legal. (2021). *Report on the implementation of specific provisions of Regulation (EU) 2016/679* [Final report]. European Commission Directorate General for Justice and Consumers Unit C.3 Data Protection. https://www.dataguidance.com/sites/default/files/1609930170392.pdf

United Nations Development Programme. (2021). *Trust in public institutions* [Policy brief]. Oslo Governance Centre. https://www.undp.org/policy-centre/governance/publications/policy-brief-trust-public-institutions/

United States Government Accountability Office. (2020). *Forensic technology: Algorithms used in federal law enforcement* (Technology Assessment No. GAO-20-479SP; Report to Congressional Requesters). https://apps.dtic.mil/sti/pdfs/AD1157070.pdf

United States Government Accountability Office. (2021). *Facial recognition technology: Federal law enforcement agencies should have better awareness of systems used By employees* (Testimony No. GAO-21-105309). https://www.gao.gov/assets/gao-21-105309.pdf

Urquhart, L., & Miranda, D. (2022). Policing faces: The present and future of intelligent facial surveillance. *Information & Communications Technology Law*, *31*(2), 194–219. https://doi.org/10.1080/13600834.2021.1994220

Valentine, S. (2019). Impoverished algorithms: Misguided governments, flawed technologies, and social control. *Fordham Urban Law Journal*, *46*(2), 364–427. https://ir.lawnet.fordham.edu/ulj/vol46/iss2/4/

Vogiatzoglou, P., & Marquenie, T. (2022). *Assessment of the implementation of the Law Enforcement Directive* (Study No. PE 740.209). European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf

Vuorensyrjä, M., Rauta, J., Hämäläinen, E., Attila, H., Koivula, J., & Ollila, P. (2023). *Poliisibarometri 2022: Kansalaisten arviot poliisin toiminnasta ja Suomen sisäisen turvallisuuden tilasta [Police barometer 2022: Citizens' assessments of police activities and the state of internal security in Finland]* (Internal security) [Report]. Ministry of the Interior Finland. https://julkaisut.valtioneuvosto.fi/handle/10024/165026

Walker, L. (2023, June 14). World first: European Parliament votes for ban on AI facial recognition. *The Brussels Times*. https://www.brusselstimes.com/553065/world-first-european-parliament-votes-for-full-ban-on-ai-facial-recognition

Wang, Y.-F., Chang, E. Y., & Cheng, K. P. (2005). A video analysis framework for soft biometry security surveillance. *Proceedings of the Third ACM International Workshop on Video Surveillance & Sensor Networks*, 71–78. https://doi.org/10.1145/1099396.1099412

Zalnieriute, M. (2024). Facial recognition surveillance and public space: Protecting protest movements. *International Review of Law, Computers & Technology*, 1–20. https://doi.org/10.1080/13600869.2023.2295690

Züger, T., & Asghari, H. (2023). AI for the public. How public interest theory shifts the discourse on AI. *AI & Society*, *38*(2), 815–828. https://doi.org/10.1007/s00146-022-01480-5

Published by

Alexander von Humboldt Institute for Internet and Society

CAIS Research for the Digital Age

in cooperation with

CREATe

cnrs centre internet et société

UOC R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies